TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de viabilidad mediante un caso de negocio en el Departamento de Tecnologías de Información para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013 en la empresa Mobilize.NET

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Elaborado por: Bryan Daniel Blanco Morales

Prof. Tutor: Carlos Luis Mata Montero

Cartago, Costa Rica

II Semestre

Noviembre, 2021

ati

Hoja de Aprobación

TEC | Tecnológico de Costa Rica

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información recomendamos que el presente Informe Final de Proyecto de Graduación del estudiante Bryan Blanco Morales sea aceptado como requisito para obtener el grado académico de Licenciatura en Administración de Tecnologías de Información.

Jose David Chaverri Perez

José David Chaverri Pérez
Lector de la Industria

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.26 11:05:33 -06'00'

Laura Alpizar Chaves
Lector Académico

CARLOS LUIS MATA MONTERO (FIRMA)
Firmado digitalmente por CARLOS LUIS MATA MONTERO (FIRMA)
Fecha: 2021.11.26 11:24:20 -06'00'

Carlos Luis Mata Montero
Profesor Tutor

TEC | Tecnológico de Costa Rica
Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2021.11.30 09:45:26 -06'00'

Yarima Sandoval Sánchez
Coordinadora del Proyecto de Graduación

Resumen

El siguiente proyecto consiste en desarrollar una propuesta que permita alinear el Sistema de Gestión de la Seguridad de la Información (SGSI) a la norma ISO 27001:2013 para preparar adecuadamente al Departamento de TI en la empresa Mobilize.NET con miras a obtener la respectiva certificación.

Para llevar a cabo la propuesta se utiliza una metodología de investigación de enfoque mixto con diseño de triangulación concurrente para lograr un análisis y evaluación de los datos semicuantitativos obtenidos a partir de las entrevistas, reuniones observación de campo y revisión documental realizadas para desarrollar la propuesta que brinde las acciones de mejora necesarias para atender las brechas críticas identificadas en el proceso de gestión de seguridad de la información.

Palabras clave: ISO, COBIT, Certificación, Seguridad de la Información, Tecnologías de Información.

Abstract

The next project consists of developing a proposal that allows aligning the Information Security Management System (ISMS) to the ISO 27001:2013 standard to prepare the IT Department in the company Mobilize.NET, with a view to obtaining the respective certification.

To carry out the proposal, a mixed-approach research methodology with concurrent triangulation design is used to achieve an analysis and evaluation of the semi-quantitative data obtained from interviews, field observation meetings and documentary review carried out to develop the proposal that provides the necessary improvement actions to address the critical gaps identified in the information security management process.

Keywords: ISO, COBIT, Certification, Information Security, Information Technology.

Dedicatoria

A mis padres,

Leandro Blanco Gamboa y Noily Morales Cordero que gracias a sus consejos y valores inculcados me brindaron el apoyo necesario a lo largo de mi vida para desarrollar las capacidades que me permitieron superar todas las dificultades a lo largo de mi etapa académica. A ellos les dedico este logro tan importante que siempre soñé alcanzar y por el cual les estaré eternamente agradecido. Nunca olvidaré sus enseñanzas y valores, serán siempre los pilares a lo largo de mi vida.

A mis hermanos,

Josué y Diana Blanco Morales que con su amor y personalidad lograron inspirarme y brindarme su apoyo para saber que con esfuerzo y dedicación podemos alcanzar las metas que nos propongamos.

A mi familia,

Abuelos, tíos y primos que de alguna u otra manera siempre estuvieron pendientes de mis estudios, brindando la motivación y el apoyo familiar necesario para conseguir este objetivo. Gracias por el ejemplo y la humildad que siempre me han inculcado para trabajar por los sueños, lo llevaré presente siempre en mi vida.

A mí mismo,

Por demostrarme que los únicos limites que existen son los que nos ponemos nosotros mismos y a pesar de que culmino una de las etapas más exigentes y difíciles en mi vida también fue la etapa que me enseñó a romper mis propias barreras y crecer tanto personal como profesionalmente.

Agradecimientos

A mi tutor,

Carlos Mata Montero por su paciencia y dedicación para transmitir el conocimiento que hizo posible el desarrollo de este proyecto.

A mis mentores,

Paola Solano Castro y Javier Araya Hidalgo que con mucha empatía me brindaron siempre las herramientas necesarias para desarrollar el presente proyecto y me permitieron iniciar con mi experiencia profesional.

A mis profesores,

Aquellos que estuvieron presentes en los diferentes cursos de la carrera que siempre me brindaron su apoyo y me transmitieron su conocimiento para lograr ser el profesional soy y graduarme de una carrera que desde un inicio me cautivó.

A todos y todas, muchas gracias.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

Nota Aclaratoria

Género[1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del "género inclusivo". Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

Capítulo I: Introducción

La correcta gestión de la seguridad de la información en empresas que brindan servicios relacionados con las tecnologías de información es un tema de suma importancia, principalmente con el aumento presentado en las amenazas informáticas a causa de la pandemia por la Covid-19, por esta razón las empresas buscan mantenerse a la vanguardia para cumplir con los protocolos que aseguren la adecuada gestión de datos e información sensible (INTERPOL, 2020).

Cuando se habla de seguridad de la información se pueden encontrar diferentes definiciones, para efectos de este trabajo se toma como referencia la definición emitida por el estándar ISO 27000 publicado por International Organization for Standardization (ISO) y por International Electrotechnical Commission (IEC) en el año 2018, que dice: “Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades, como autenticidad, responsabilidad, no repudio y confiabilidad también pueden estar involucradas”.

Por lo tanto, se puede hablar de seguridad de la información si se cumple con preservar estos tres principios fundamentales: confidencialidad, integridad y disponibilidad.

Mobilize.Net ayuda a las empresas que requieren de una actualización de sus activos de software, ofreciendo la posibilidad de dotar las aplicaciones y herramientas digitales de sus clientes con las últimas tecnologías. Para conseguir esto es necesario realizar una migración de software, implicando que los clientes deban facilitar el código fuente a Mobilize.Net, es aquí donde la seguridad se vuelve un aspecto de gran valor para los clientes, los cuales buscan contratar a empresas que se encarguen de realizar dicha migración, cumpliendo con los requerimientos establecidos por estándares internacionales que garanticen la seguridad de la información y el resguardo de su propiedad intelectual.

1.1. Descripción General

Con el desarrollo de este proyecto se pretende determinar la viabilidad de obtener una certificación en la gestión de la seguridad de la información con la norma ISO 27001:2013 a partir del desarrollo de un caso de negocio que permita identificar los pasos a seguir por el Departamento de TI, tomando en cuenta los requerimientos que se reciben por parte de los clientes y la organización así como las necesidades del negocio.

Esto permitirá a la organización contar con respaldos y garantías acreditadas en la seguridad de la información que brinden mayor confianza a sus clientes y que le permita a la empresa ofrecer servicios de calidad, bajo estándares que aseguren la correcta gestión de la seguridad de la información.

Además ofrece a los colaboradores de la organización nuevos conocimientos y habilidades que se traducen en una mayor agilidad en los procesos al momento de implementar buenas prácticas que permitan disminuir los riesgos e incidentes.

En la estructura de este trabajo se mencionan detalladamente los aspectos que serán necesarios a tomar en cuenta para el desarrollo de este proyecto financiado por la empresa Mobilize.Net.

1.2. Antecedentes

Con el desarrollo de este apartado se pretende contextualizar mejor acerca de la empresa Mobilize.Net con su respectiva misión, visión y valores. También se presenta el equipo de trabajo y Departamento de TI donde se desarrolla el proyecto, así como algunos trabajos similares realizados de forma interna o externa que serán tomados como referencia.

1.2.1. Descripción de la Organización

Mobilize.Net es una empresa fundada en Costa Rica que nació a partir de un emprendimiento, Federico Zoufaly co-fundador de la empresa menciona en un video de la organización: "empezamos con una idea hace más de veinticinco años en una finca de café, allá en Cartago, que es nuestra versión del garaje de Silicon Valley" *MobilizeNet.* (2021).

El objetivo de esa idea era brindar la posibilidad a diferentes empresas de aprovechar el conocimiento que habían adquirido en sus plataformas y software realizando una actualización de las aplicaciones migrando hacia nuevos lenguajes que cuentan con mejores tecnologías, lo que permite a estas empresas mantenerse a la vanguardia sin requerir de la adquisición o desarrollo de nuevo software.

Actualmente la empresa mantiene su idea inicial como su principal estrategia, lo que les ha permitido crecer a nivel mundial, trabajando con empresas en alianza como Microsoft y Snowflake que les permiten ofrecer a sus clientes servicios de alta calidad en la migración de sus plataformas *MobilizeNet.* (2021).

Cuenta con dos oficinas, la principal se encuentra ubicadas en Bellevue, Seattle, Estados Unidos y una segunda en La Sabana, Costa Rica; en total cuenta con aproximadamente doscientas personas en sus diferentes equipos de trabajo dentro de sus departamentos, los cuales se detallan más adelante en el organigrama de la empresa.

A continuación se detallan la misión, visión y valores promovidos por la empresa Mobilize.Net.

1.2.1.1. Misión

La misión de la empresa se define a continuación.

"Somos una empresa líder en el mercado reconocida por eficiencia y calidad en migraciones de software".

1.2.1.2. Visión

En cuanto a la visión la empresa establece la siguiente.

"Ser la empresa de preferencia del cliente en migraciones de software a nivel mundial".

1.2.1.3. Valores

La empresa se preocupa por inculcar en sus colaboradores una serie de valores de gran importancia para su estrategia organizacional, los cuales se detallan a continuación.

Smart: inventamos soluciones creativas para problemas difíciles que mejoran continuamente nuestra tecnología, procesos y personas.

Team Oriented: colaboramos compartiendo conocimiento, ideas y esfuerzos para garantizar que el equipo tenga éxito. Ayudamos a los compañeros de equipo.

Agile: implementamos nuestras decisiones de inmediato para que tengamos éxito o fracasemos rápidamente, aprendemos y corregimos el curso rápidamente.

Nice: nos preocupamos por las personas. Estamos comprometidos en hacer de Mobilize un lugar emocionante, divertido y productivo donde a personas maravillosas les encante trabajar.

Driven: Hacemos lo que sea necesario para lograr nuestros objetivos. Somos persistentes y tenaces.

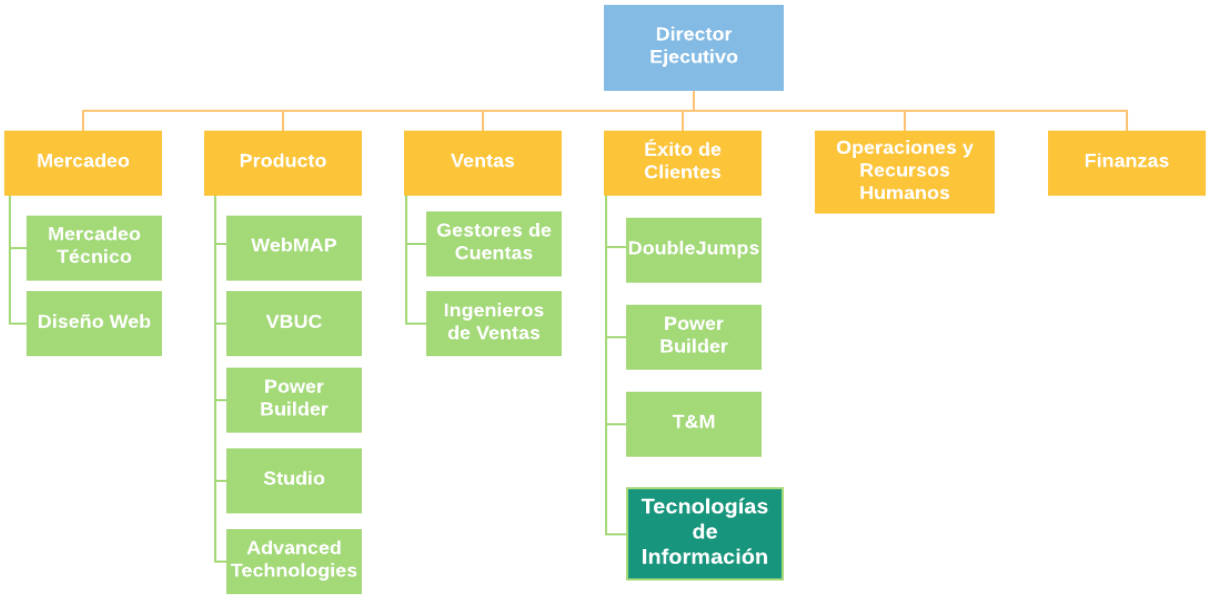
Unfiltered: decimos la verdad de forma honesta, comunicando hechos objetivos, malos o buenos inmediatamente de forma constructiva.

Passionate: amamos lo que hacemos y entregamos productos de calidad de los que estamos orgullosos.

1.2.1.4. Equipo de Trabajo

En esta sección se detalla acerca de la organización y el equipo de trabajo con el que se va a desarrollar el proyecto. En la siguiente **Figura 1** se muestra el organigrama de la empresa.

Figura 1
Organigrama de Mobilize.Net



Fuente: Adaptación del Plan Estratégico.

El proyecto será realizado específicamente en el departamento de Tecnologías de Información (TI), el cual será el principal beneficiado, sin embargo, al tratarse de una propuesta enfocada en la gestión de la seguridad de la información, el beneficio también se verá reflejado en otros departamentos de la organización.

Actualmente el departamento de TI cuenta con tres principales funciones que corresponden a: Coordinación de TI, Análisis del Negocio y Soporte Técnico. En la siguiente **Figura 2** se muestra de forma gráfica la organización del departamento.

Figura 2 *Organigrama del departamento de TI*

En cuanto al equipo de trabajo se muestran los roles y puestos que desempeña cada uno de los colaboradores dentro del departamento y en su participación en el proyecto como tal en la siguiente **Tabla** 1.

Tabla 1 *Equipo de trabajo*

Cargo que desempeña	Descripción	Rol en el proyecto
Asesor de TI	Encargado de la coordinación de los proyectos y tareas dentro del departamento así como de la toma de decisiones y la administración de adquisiciones.	Patrocinador

Cargo que desempeña	Descripción	Rol en el proyecto
Analista de negocio	Responsable de la implementación de cambios en la infraestructura de TI, soporte de tecnologías en la nube y locales. Responsable de la ejecución de la calidad de los procesos operativos y asegurar la continuidad constante del servicio a través del soporte y la gestión de aplicaciones y sistemas comerciales críticos. Responsable de administrar el presupuesto de TI de acuerdo al costo / beneficio de los proyectos y los requerimientos del negocio.	Mentor
Analista de Negocio CRM	Encargado de investigar y recopilar datos relacionados con los diferentes clientes de la empresa para generar nuevas estrategias o reportes que permitan fortalecer relaciones y generar nuevas oportunidades de venta. Además, brinda apoyo en la creación y mejora de procesos internos.	Mentor
Soporte Técnico	Responsables de brindar soporte a diferentes áreas tanto a lo interno de la organización como a los usuarios finales en la plataforma de trabajo.	Colaborador
Desarrollador del proyecto	Practicante dedicado a la gestión de la seguridad de la información.	Desarrollador del proyecto

1.2.2 Trabajos Similares Realizados Dentro y Fuera de la Organización

En esta sección se describen algunos trabajos similares realizados previamente que pueden funcionar como una base inicial que funcione como referencia para el desarrollo de este proyecto.

1.2.2.1. Propuesta de Mejora para la Gestión de Seguridad del Centro de Datos. Es importante mencionar que, de manera interna, solo existe un trabajo relacionado con este proyecto, el cual fue desarrollado en Mobilize.Net en el año 2017 por la Lic. Andrea Paola Solano Castro como parte de su trabajo final de graduación. El proyecto estableció los primeros pasos tomados por la empresa en la gestión de la seguridad enfocada en su centro de datos y se pretende que sea un insumo que brinde un gran aporte al desarrollo de este proyecto.

1.2.2.2. Contenido de Seguridad en el Grado de Informática Acorde con las Certificaciones Profesionales.

El objetivo de este proyecto fue implementar una serie de criterios en seguridad de información en diferentes asignaturas, en el desarrollo del documento los autores García et al. (2014), realizan un análisis comparativo de diferentes estándares internacionales lo cual servirá como una guía o referencia para el estudio de dichos estándares.

1.2.2.3. Metodología Para la Implementación de un Sistema de Gestión de Seguridad de la Información Basada en la Familia de Normas ISO/IEC 27000.

En este trabajo realizado por Valencia y Orozco (2017), se presenta una propuesta para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en las normas de la familia ISO/IEC 27000 a través de las que se desarrollan las actividades necesarias para cumplir con los requerimientos establecidos por el estándar.

1.2.2.4. Propuesta de un Sistema de Gestión de la Seguridad de la Información Para Entidades Dedicadas al Servicio de Outsourcing de TI.

Esta propuesta de los autores Guerrero y Martínez (2016), presenta la implementación de un Sistema de Gestión de Seguridad de la Información enfocado en empresas que brindan servicios de outsourcing basándose en las normas ISO/IEC 27001 y la metodología Magerit, lo que representa un insumo de gran importancia por las características similares que tiene en su aplicación a la empresa Mobilize.Net.

1.3. Planteamiento del Problema

En esta sección se detallan las diferentes situaciones presentadas que especifican de manera más clara el fondo del problema así como posibles causas asociadas a la necesidad de desarrollar este proyecto por parte de la empresa.

1.3.1. Situación Problemática

La empresa Mobilize.NET identificó como una de sus necesidades brindar mayor seguridad a sus clientes en el proceso de migración, principalmente en la visión a futuro de optar a la certificación en la norma ISO 27001:2013 correspondiente a la gestión de la seguridad de la información en la búsqueda de contar con los controles que permitan garantizar un tratamiento de calidad a los activos de software de las empresas que contratan los servicios de Mobilize.Net.

A partir de esto se identifica que el origen de las condiciones actuales de la seguridad de la información en los procesos de migración, se generan por el Departamento de TI, encargado de la gobernanza y la regulación de la seguridad de la información a través de la infraestructura de TI disponible en la organización.

Dentro de los indicadores clave de rendimiento planteados por el departamento de Tecnologías de Información se establece la necesidad de crear mecanismos que permitan mejorar las medidas de seguridad a partir de soluciones inteligentes que transmitan la confianza necesaria a los clientes al momento de trabajar con sus datos, como se muestra en la siguiente **Tabla 2**.

Tabla 2 *Objetivos e indicadores clave de rendimiento del Departamento de TI.*

Objetivo del departamento	Rol	Objetivo del responsable	Descripción	Indicador
Enviar proyectos de clientes a tiempo y con calidad	Asesor de TI	Organización de TI	Ejecutar la estrategia en nuestra pila de tecnología de TI, como lo es, seguridad, continuidad del negocio y ejecución.	Dashboard del proyecto, reportes financieros del proyecto, plan de entrega del proyecto, plan de ejecución del proyecto, informe LoC / h
		Eficiencia en la ejecución	Buscar continuamente formas de optimizar la eficiencia en los procesos de trabajo	Al menos el 95% de las tareas / asignaciones individuales se completaron sin regresiones ni errores informados por el cliente debido a nuevas implementaciones.

Objetivo del departamento	Rol	Objetivo del responsable	Descripción	Indicador
			y asegurándose de evitar cualquier tipo de regresiones.	
	Analista de negocio	Seguridad	Crear mecanismos para mejorar las medidas de seguridad y la IP de clientes.	Soluciones inteligentes para asegurar a nuestros clientes y potenciales clientes que sus datos están seguros con nosotros. Definir metodologías específicas para brindar esta información al cliente de una manera ágil y salir de cualquier tecnología heredada en los servicios que brindamos. Obtener comentarios de clientes o auditorías de clientes para implementar en nuestra organización, busque cosas pequeñas que generen el mayor impacto.
Satisfacción de clientes	Analista de negocio	Ejecución	Asegurar la ejecución de manera oportuna, priorizar contra la criticidad y el impacto.	Satisfacción del cliente. Mejora de la cobertura de tecnologías. Proporcione soluciones listas para usar para problemas complejos. Coordinar recursos para lograr resultados (ALBATROS). Gestión de hardware en todas las organizaciones.

Fuente: Indicadores clave de rendimiento del Departamento de TI (ver **Apéndice E. Indicadores Clave de Rendimiento del Departamento de TI**.).

Actualmente, la empresa recibe los requerimientos de sus clientes a través de un cuestionario y se analizan con base en diferentes marcos de referencia que ofrecen controles en relación al requerimiento solicitado. Sin embargo, no se cuenta con una estandarización definida ni tampoco se han establecido los lineamientos base que le permitan a la organización y sus colaboradores evaluar de manera efectiva sus procesos.

Javier Araya, analista de negocio en Mobilize.Net, en una entrevista realizada indicó “Muchas veces lo que hacemos es recibir el cuestionario de clientes y, en conjunto con la tabla de equivalencias, se evalúa manualmente cuáles controles se cumplen y cuáles no” (Araya.J., comunicación personal, 29 de julio, 2021).

Aunado a esto, la empresa ha identificado un incremento en los requerimientos recibidos por parte de sus clientes, como lo menciona la analista del negocio Paola Solano, “Hemos notado que los clientes están cada vez más rigurosos en la parte de seguridad y no queremos que esto llegue a ser un impedimento.” (Solano,P., comunicación personal, 23 de julio, 2021).

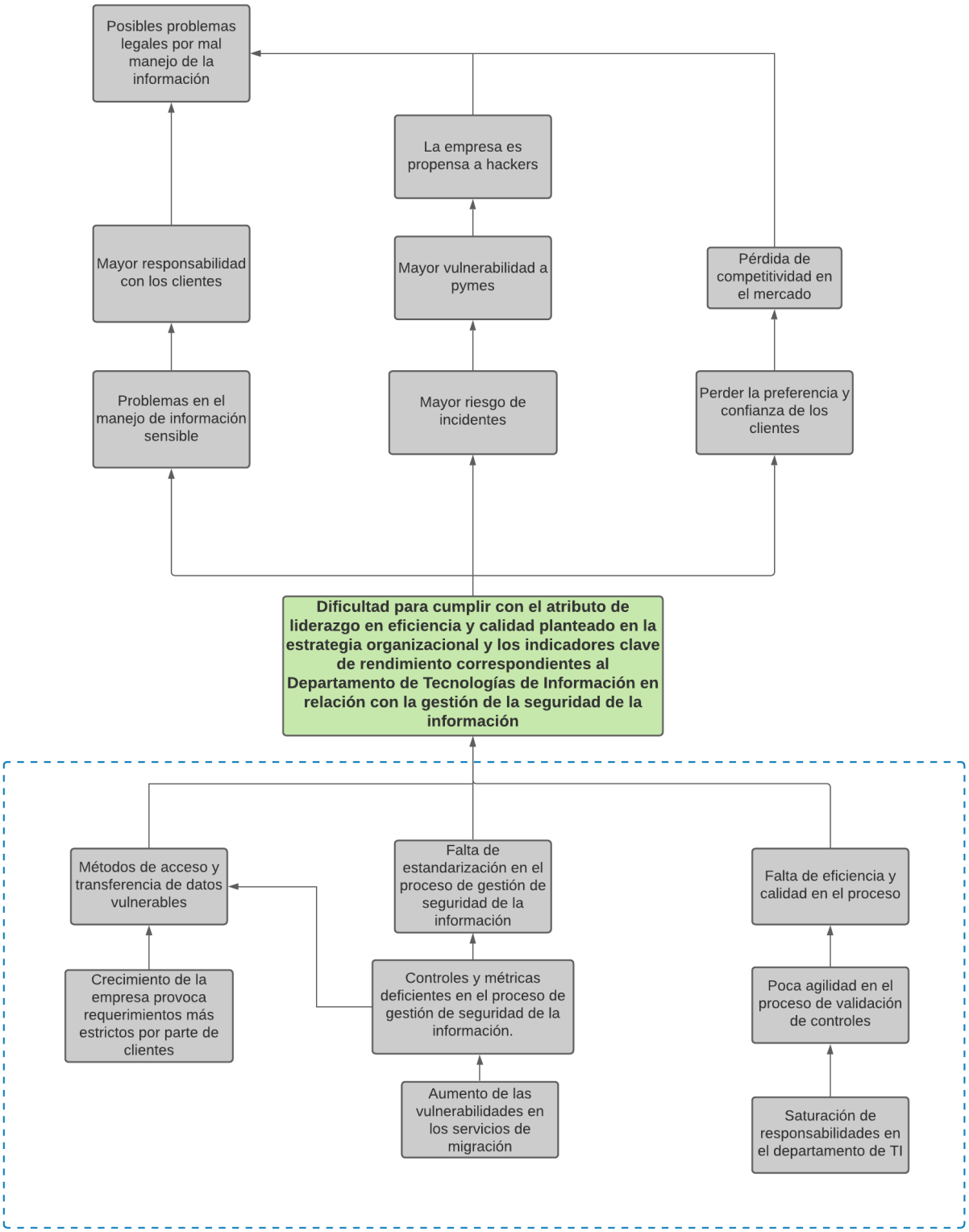
Estos aspectos han puesto en riesgo algunos de los objetivos estratégicos de la empresa, en relación con la calidad y efectividad de sus procesos y el deseo de mantener la preferencia de sus clientes en los servicios de migración que ofrece Mobilize.Net.

A falta de una persona encargada de implementar estos controles, la empresa decide destinar el presupuesto necesario para poner en marcha este proyecto, el cual, busca establecer los pasos a seguir en la adecuada gestión de la seguridad de la información bajo la norma ISO 27001 que le permitan obtener una certificación en esta área, estableciendo los controles internos necesarios en el cumplimiento de métricas y criterios que garanticen a sus clientes procesos de calidad en la migración de software.

Además, se requiere un mayor nivel de capacidad en las áreas de la organización, lo cual se desea obtener al implementar una estandarización que garantice un proceso adecuado en la gestión de seguridad de la información. Para esto se requiere dotar de nuevos conocimientos y habilidades a los colaboradores de la organización que, al ser aplicados, brindarán mayor calidad y agilidad en los procesos dentro de las diferentes áreas y departamentos en la empresa.

En la siguiente **Figura 3** se muestra gráficamente a partir de un árbol de problema las causas y efectos del problema principal.

Figura 3 Árbol del problema


Posibles problemas legales por mal manejo de la información
La empresa es propensa a hackers
Mayor responsabilidad con los clientes
Mayor vulnerabilidad a pymes
Pérdida de competitividad en el mercado
Problemas en el manejo de información sensible
Mayor riesgo de incidentes
Perder la preferencia y confianza de los clientes
Dificultad para cumplir con el atributo de liderazgo en eficiencia y calidad planteado en la estrategia organizacional y los indicadores clave de rendimiento correspondientes al Departamento de Tecnologías de Información en relación con la gestión de la seguridad de la información
Métodos de acceso y transferencia de datos vulnerables
Falta de estandarización en el proceso de gestión de seguridad de la información
Falta de eficiencia y calidad en el proceso
Crecimiento de la empresa provoca requerimientos más estrictos por parte de clientes
Controles y métricas deficientes en el proceso de gestión de seguridad de la información.
Poca agilidad en el proceso de validación de controles
Aumento de las vulnerabilidades en los servicios de migración
Saturación de responsabilidades en el departamento de TI

Al concluir este proyecto se pretenden determinar las diferentes limitantes que presenta el Departamento de TI para contar con los requerimientos que le permitan optar a certificar el proceso de gestión de seguridad de la información, realizando los análisis necesarios y definiendo las brechas que requieren ser atendidas.

1.3.2. Justificación del Proyecto

Con el desarrollo de este proyecto se pretende aplicar diferentes conocimientos adquiridos a lo largo de la carrera los cuales permitirán a la empresa obtener beneficios que atacarán directamente sus principales necesidades, una de estas corresponde con abordar el tema de la seguridad de la información.

En los últimos meses se ha presentado un aumento en los ataques y riesgos relacionados con la seguridad de sus sistemas, principalmente a causa de la pandemia y el teletrabajo. Félix Barrio Juárez, director del Hub de Ciberseguridad del Tec de Monterrey, expresó para la revista Forbes México lo siguiente:

La afluencia masiva de empresas, particularmente pequeñas y medianas empresas con poca preparación cibernética, a los servicios digitales a distancia durante el periodo de confinamiento, eleva el umbral de fragilidad de nuestra economía digital. Mientras la gran empresa lleva tiempo preparándose en términos de ciberseguridad, la abrumadoramente mayoritaria pyme requiere de un plan estratégico a nivel estatal que combine campañas de concientización, acciones de capacitación y ayudas a la inversión que le faciliten la necesaria preparación ante este cúmulo de amenazas cibernéticas. (Barrio, 2020)

La seguridad de la información es un tema de gran importancia en la actualidad, principalmente en una empresa como Mobilize.Net, donde trabajan con una gran cantidad de datos de sus clientes. Tomar acciones en torno a la estandarización de los procesos que permitan al Departamento de TI generar los controles necesarios implica, para el desarrollador

del proyecto, la necesidad de abordar una serie de conocimientos adquiridos a lo largo de la carrera que le permitirán obtener una experiencia de la teoría aplicada, considerando las preocupaciones que se tienen actualmente en la industria.

La norma ISO / IEC 27001:2013 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 (ISO, 2013).

Para Mobilize.Net es vital que su sistema de gestión de la seguridad de la información se adapte a su contexto y objetivos estratégicos, tomando en cuenta los diferentes involucrados y requerimientos que influyan en la organización.

El desarrollo de este proyecto será un paso inicial en la búsqueda de asegurar la estandarización del proceso de gestión de la seguridad de la información, de manera que el Departamento de TI tenga un panorama claro de la situación actual y el camino a seguir para implementar la propuesta que le permita cumplir con los requerimientos establecidos para la certificación.

Obtener una acreditación es una oportunidad de gran valor para la organización en la necesidad estratégica de mantener la preferencia, confianza y satisfacción de sus clientes, los cuales buscan en los servicios de migración el cumplimiento de todas las medidas en seguridad de la información. Asegurar dichos cumplimientos permitirá mantener la calidad en los servicios que ofrece Mobilize.Net, lo que se traduce en mayor competitividad dentro del mercado al que pertenece.

Para determinar los aspectos técnicos, estratégicos y de gestión que deben ser evaluados se realizarán diferentes estudios que permitan analizar el Departamento de TI desde una perspectiva interna, donde se conozcan sus procesos y se establezcan las acciones a tomar para alinear dichos procesos al cumplimiento de la norma ISO 270001:2013.

Además, el desarrollo de este proyecto responde directamente con los objetivos e indicadores clave de rendimiento del Departamento de Tecnologías de Información, presentados anteriormente en la **Tabla 2**, los cuales expresan la necesidad de crear soluciones inteligentes para satisfacer a sus clientes garantizando que sus datos se encuentran seguros, así como definir metodologías específicas en materia de seguridad de la información que permitan la estandarización del proceso.

1.3.3. Beneficios Esperados o Aportes del Trabajo Final de Graduación

Con el desarrollo de este proyecto se pretende ofrecer a la empresa Mobilize.Net una serie de beneficios que le permitirán crecer como organización y mejorar las capacidades de sus colaboradores. Algunos de los beneficios más importantes se detallan a continuación.

1.3.3.1. Identificación de Nuevos Requerimientos. Al identificar una mayor rigurosidad en los requerimientos enviados por los clientes, los cuales serán tomados en cuenta para el desarrollo de este proyecto, se pretende establecer las prioridades de atención de acuerdo con las brechas encontradas y las principales preocupaciones de los clientes.

1.3.3.2. Alineamiento de Políticas en Seguridad con el Estándar ISO 27001:2013. Alinear las políticas de seguridad de la información a un estándar específico permite a la empresa garantizar la calidad en sus servicios de migración de datos al mismo tiempo que brinda una mayor agilidad en los procesos y facilita su control.

1.3.3.3. Disminución en los Riesgos de Implementación. Al presentar un plan de implementación respaldado por los diferentes análisis y estudios, realizados previamente, se busca ofrecer un panorama claro del camino que la empresa debe seguir en el objetivo planteado evaluando los posibles riesgos de obtener la futura certificación.

1.3.3.4. Disminución de los Riesgos. Estandarizar el proceso de gestión de seguridad de la información permite disminuir los riesgos asociados y mantener un mejor control de las operaciones por parte del Departamento de TI.

1.4. Objetivos del Trabajo Final de Graduación

En esta sección se definen los objetivos, tanto el general como los específicos, los cuales determinarán las tareas a realizar en el desarrollo del proyecto.

1.4.1. Objetivo General

Elaborar una propuesta de viabilidad mediante un caso de negocio en el Departamento de Tecnologías de Información para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013, en un periodo de dieciséis semanas para la empresa Mobilize.NET.

1.4.2. Objetivos Específicos

- Analizar la situación actual del Departamento de TI en relación con la identificación de controles en seguridad de la información necesarios y el cumplimiento de los requerimientos recibidos.
- Establecer los aspectos estratégicos, técnicos y de gestión necesarios para el desarrollo de la propuesta.
- Desarrollar los estudios de factibilidad necesarios que permitan determinar la viabilidad de la certificación.
- Elaborar una propuesta de implementación que brinde la guía necesaria para obtener la certificación en ISO 27001:2013 para el departamento de TI en la empresa.

1.5. Alcance del Proyecto

Para el desarrollo de este proyecto se pretende determinar la viabilidad de obtener una certificación en el proceso de gestión de la seguridad de la información, alineada al estándar internacional ISO 27001:2013, el cual permita al Departamento de TI establecer los controles necesarios en el cumplimiento de los requerimientos en seguridad de la información presentados por los clientes de la empresa. Además, se presentará un plan de implementación y un cronograma a seguir que permitan la futura ejecución de la propuesta, la cual estará definida para el Departamento de Tecnologías de Información y la infraestructura tecnológica sobre la que es responsable el Departamento.

A continuación se detallan los aspectos que se tomarán en cuenta para el desarrollo del proyecto así como los detalles que quedarán por fuera del alcance planteado.

1.5.1. Elementos a Incluir

Para cumplir con los diferentes objetivos planteados se realizará una división del trabajo en diferentes fases que se detallan a continuación.

1.5.1.1. Fase I: Análisis de la Situación Actual. Como primer paso para el desarrollo de este proyecto se requiere tener el contexto de la organización, para esto se realiza un análisis de la situación actual del Departamento de TI que permita conocer trabajos realizados previamente en la organización, de forma que el proyecto brinde los aspectos necesarios por tomar en cuenta para obtener la certificación.

Para lograr un panorama claro de la organización se identifican los requerimientos solicitados por los clientes, a través de un análisis matricial que permita conocer las preocupaciones generales que se presentan en seguridad de la información. Además se identifican los controles que el Departamento de TI implementa actualmente en relación con el estándar ISO 27001:2013 para determinar el estado actual del proceso de gestión de la

seguridad de la información, de esta forma se planea identificar los controles y métricas faltantes en los procesos de la empresa que requieran ser implementados para optar por una certificación.

1.5.1.2. Fase II: Formulación. Una vez se tenga el contexto de la organización se plantea, como siguiente paso, realizar la formulación de la propuesta en torno a la seguridad de la información, para esto se define el SGSI basado en la norma ISO 27001:2013, donde se identifican los controles aplicables a la organización y se verifican cada uno de ellos para determinar su estado actual y nivel de cumplimiento por área.

De esta forma se pretende definir las acciones necesarias para atacar las brechas identificadas que permitan el alineamiento de los procesos de la empresa con los requerimientos necesarios para la certificación.

Para concluir con esta etapa se pretende determinar los niveles de capacidad en cada una de las áreas que permita conocer el estado actual y determinar la priorización de las brechas que serán atacadas, estableciendo el nivel de capacidad al que se desea llegar con la implementación de la propuesta.

1.5.1.3. Fase III: Evaluación a Partir del Caso de Negocio. Al conocer en qué punto se encuentra la organización y sabiendo los requerimientos necesarios para la certificación, se realizarán los estudios y análisis correspondientes que permitan evaluar la propuesta presentada y conformar el caso de negocio para determinar la viabilidad del proyecto.

1.5.1.4. Fase IV: Plan de Implementación. Por último, tenemos la fase que comprende el plan de implementación el cual contendrá los pasos a seguir en la futura ejecución del caso de negocio planteado en la fase anterior.

1.6. Supuestos del Proyecto

Algunos elementos que se consideran como un hecho para la realización de este proyecto son:

Al menos un 80% de la información necesaria se encuentra documentada por la empresa.

El trabajo desarrollado en cuanto a la seguridad de los centros de datos se encuentra alineado a la realidad de la organización.

La organización cuenta con la madurez necesaria para la futura implementación de la propuesta.

Se tendrá disponibilidad de los diferentes colaboradores e integrantes del equipo de trabajo para recurrir a información necesaria en el momento oportuno.

1.7. Entregables del proyecto

A continuación se definen los diferentes entregables del proyecto, los cuales serán presentados a lo largo de su desarrollo en la organización.

1.7.1. Entregables del producto

En esta sección se definirán detalladamente los diferentes entregables establecidos para el producto, los cuales se encuentran asociados a los objetivos del proyecto.

1.7.1.1. Matriz de Evaluación de la Seguridad de la Información. Con esta matriz se pretende centralizar los controles especificados por la norma ISO 27001:2013 y los controles generados a partir de los requerimientos recibidos en la empresa por parte de sus clientes, de forma que sea posible verificar el cumplimiento de controles implementados por parte de la organización y determinar las áreas y controles que requieren ser atendidos.

1.7.1.2. Análisis de brecha y capacidad. Al analizar los resultados obtenidos en la matriz de verificación se pretende determinar las brechas encontradas en las diferentes áreas de control así como el nivel de capacidad obtenido según lo establecido por COBIT 2019.

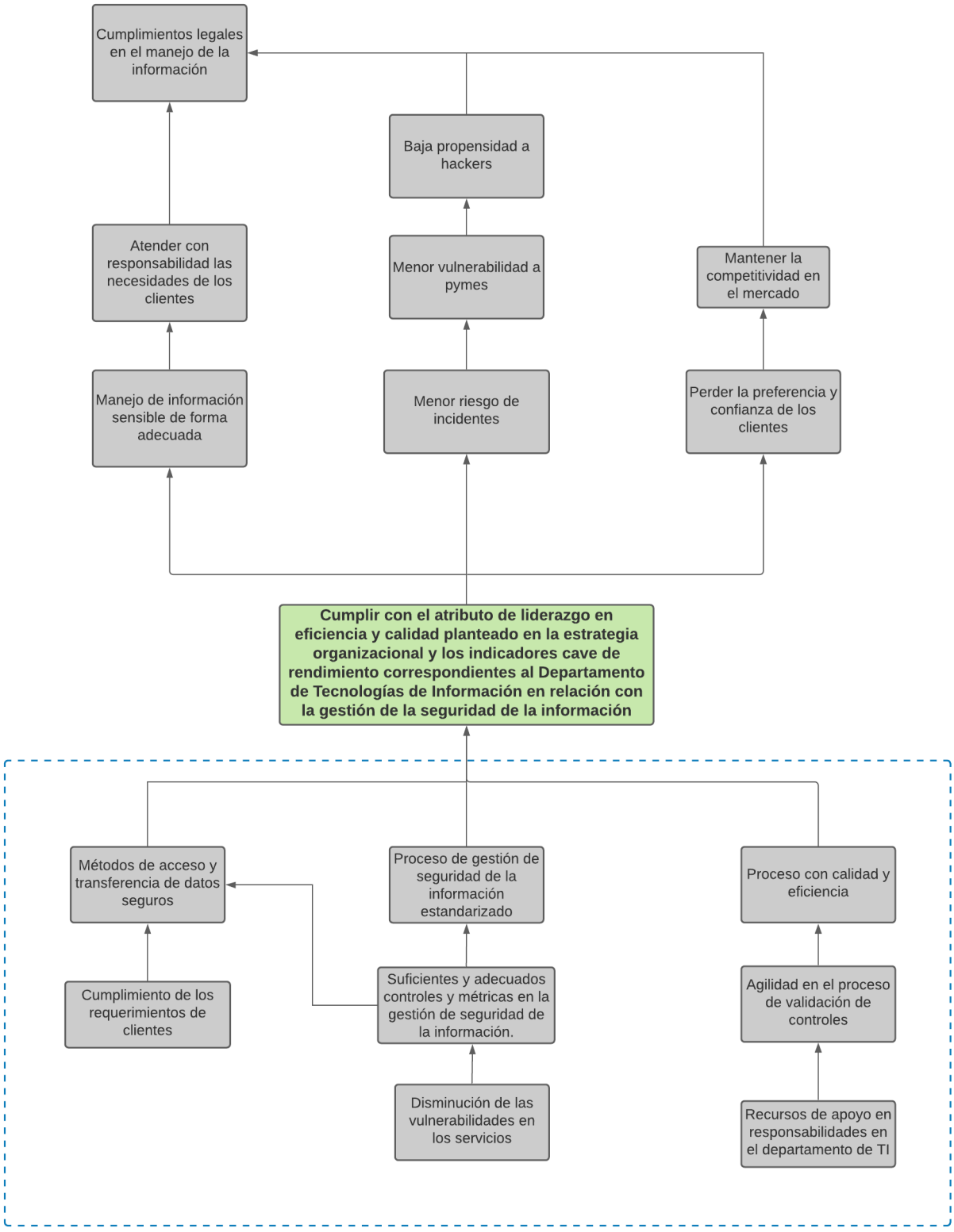
1.7.1.3. Caso de negocio. Este entregable corresponde al documento digital que contiene todos los análisis y estudios necesarios para determinar la viabilidad, de adquirir la certificación planteada.

1.7.1.4. Plan de implementación. Se desarrollará un plan de implementación en el que se especifican las acciones a tomar y los pasos a seguir por la empresa para optar por la certificación en seguridad de la información.

1.7.2 Gestión del proyecto

A continuación se presentan los documentos utilizados para el adecuado seguimiento del proyecto a lo largo de su ejecución.

1.7.2.1. Minutas. **Para mantener un control documentado de los diferentes aspectos evaluados, comentados y aprobados en las diferentes reuniones que se deben llevar a cabo durante el desarrollo del proyecto (ver Apéndice L. Árbol de Objetivos.**


Cumplimientos legales en el manejo de la información
Baja propensidad a hackers
Atender con responsabilidad las necesidades de los clientes
Menor vulnerabilidad a pymes
Mantener la competitividad en el mercado
Manejo de información sensible de forma adecuada
Menor riesgo de incidentes
Perder la preferencia y confianza de los clientes
Cumplir con el atributo de liderazgo en eficiencia y calidad planteado en la estrategia organizacional y los indicadores cave de rendimiento correspondientes al Departamento de Tecnologías de Información en relación con la gestión de la seguridad de la información
Métodos de acceso y transferencia de datos seguros
Proceso de gestión de seguridad de la información estandarizado
Proceso con calidad y eficiencia
Cumplimiento de los requerimientos de clientes
Suficientes y adecuados controles y métricas en la gestión de seguridad de la información.
Agilidad en el proceso de validación de controles
Disminución de las vulnerabilidades en los servicios
Recursos de apoyo en responsabilidades en el departamento de TI

Apéndice M. Minutas con Tutor y Apéndice N. Minutas de Reuniones con la Organización.).

1.7.2.2. Cronograma. Como parte del seguimiento del proyecto se establecen actividades que requieren ser ejecutadas, a continuación se definen a nivel general las fases de ejecución que requiere el desarrollo del proyecto.

- **Fase I: Análisis de la Situación Actual.** Se desarrollan las actividades de investigación y análisis documental que brinden el contexto de la organización y la la situación actual del Departamento de TI
- **Fase II: Formulación.** Una vez se tenga el contexto de la organización se desarrollan las actividades que permitan la formulación de la propuesta con el SGSI basado en la norma ISO 27001:2013. Además, se deben identificar las brechas que serán atacadas estableciendo el nivel de capacidad al que se desea llegar con la implementación de la propuesta.
- **Fase III: Evaluación a Partir del Caso de Negocio.** Se llevan a cabo las actividades que permitan evaluar la propuesta presentada a partir de los análisis y estudios necesarios.
- **Fase IV: Plan de Implementación.** Se definen las actividades que deben ser llevadas a cabo por cada responsable para la implementación de la propuesta planteada.

1.8. Limitaciones del proyecto

Se definen a continuación los posibles aspectos que afecten en alguna medida el desarrollo del proyecto:

a) El desarrollo de este proyecto no incluye la implementación o ejecución del mismo.

b) No se contempla dentro del desarrollo de este proyecto la implementación de capacitaciones necesarias para lograr que la organización se adapte adecuadamente la propuesta de solución.

c) Por políticas de seguridad y confidencialidad de la empresa alguna información correspondiente a las especificaciones de los activos críticos o datos financieros pueden no estar disponibles al conocimiento público en este proyecto.

Capítulo II: Marco Conceptual

En el siguiente capítulo se pretende brindar al lector una contextualización del desarrollo del proyecto, definiendo los conceptos necesarios y los marcos de referencia que serán utilizados en las diferentes etapas del mismo, estableciendo el tema en el que se enfoca y los efectos que se buscan conseguir dentro del departamento de TI de la empresa.

También se especifica lo establecido por la Organización Internacional de Estandarización (ISO, por sus siglas en inglés), que será el estándar a utilizar como marco de referencia en materia de gestión de la seguridad de la información para este proyecto.

Además, se definen los apartados de *Control Objectives for Information and related Technology* (COBIT) relacionados con la seguridad de la información, además de los niveles de capacidad especificados por el marco de referencia.

Seguidamente, se presenta lo abordado por los autores Ataya Georges y John Thorp en su documento Enterprise Value: Governance of IT Investments, The Business Case (Val IT), basado en COBIT y publicado por el IT Governance Institute (ITGI), el cual establece una guía para la elaboración de un caso de negocio, tomando en cuenta sus objetivos, etapas de aplicación, herramientas y técnicas sugeridas. (Georges & Thorp, 2007)

También se expondrán las fases propuestas por COBIT 2019 para el desarrollo de un caso de negocio donde se plantean las etapas en la gestión de un programa, las cuales servirán como referencia para el desarrollo de la propuesta de solución. (COBIT 2019 Framework: Introduction and Methodology, 2018)

2.1. Tecnologías de Información y Comunicación

Las Tecnologías de Información y Comunicación (TIC) han experimentado un crecimiento exponencial y se han convertido en un elemento fundamental de las empresas en

el último siglo al momento de gestionar sus procesos y recursos cuando se tiene una gran cantidad de información y se requiere de un tratamiento adecuado y efectivo de los datos.

Estas tecnologías de información y comunicación están constituidas por inversiones en áreas relacionadas con el tratamiento de la información, como lo pueden ser: equipos computacionales, medios de comunicación y software (Alderete & Gutiérrez, 2012).

Emplear las TICs de manera adecuada permite a las empresas contar con herramientas que generen un aumento en la productividad y competitividad; siempre y cuando se mantenga una correcta innovación empresarial, una ejecución óptima de los procesos y estrategia, así como la inversión en su capital humano e intelectual («Nuevas Tecnologías & Innovación», 2007)

Por lo tanto, hacer un uso adecuado de las TIC permite a las organizaciones aprovechar las posibilidades que le brindan las diferentes herramientas en sus procesos internos, principalmente en empresas que se encuentran en crecimiento y requieren de sistemas que les permitan gestionar la información y comunicación de manera efectiva.

Las tecnologías de información y comunicación son un recurso de gran valor para las organizaciones en la actualidad, conocer sus posibilidades y trabajar con ellas para mejorar los diferentes procesos permite un crecimiento en áreas técnicas, estratégicas y de gestión dentro de las empresas.

Alderete y Gutiérrez (2012) concluyen en su estudio que las tecnologías de información y comunicación juegan un papel de suma importancia al momento de ofrecer servicios de calidad a los clientes, evidenciando una relación significativamente positiva entre las inversiones de capital en TIC, las aplicaciones informáticas y la productividad laboral de los servicios.

2.2. Seguridad de la Información

La seguridad de la información se puede definir como un conjunto de prácticas y controles que mantengan los datos seguros de alteraciones y accesos no autorizados. Según lo establece ISO/IEC 27000, la seguridad de la información busca la preservación de la confidencialidad, integridad y disponibilidad de la información (Blokdyk, 2017).

Por su parte, Gartner se refiere a la ciberseguridad como la integración de personas, políticas, procesos y tecnologías utilizadas por una empresa para proteger sus activos digitales, incluidos dentro de ellos la información y datos (Gartner Information Technology Glossary, s. f.).

Tomando en cuenta las definiciones anteriores, este proyecto pretende analizar las diferentes prácticas y controles en la seguridad de la información que se aplican en la organización, así como aquellos controles que sean necesarios de implementar, tomando en cuenta los recursos, personas y tecnología con la que cuenta la infraestructura del departamento de TI.

2.3. Gobernanza de TI

El constante cambio en el mercado que se vive actualmente a raíz del crecimiento acelerado de las tecnologías, ha provocado que las empresas dediquen mayores esfuerzos en mantener una gobernanza en el desarrollo de sus funciones que permita medir, controlar y destinar los recursos necesarios para cada uno de sus proyectos de una manera efectiva, además de gestionar los riesgos adecuadamente para evitar que se provoquen impactos significativos en el transcurso de los mismos.

La gobernanza de TI es un sistema que permite controlar el uso, actual y futuro, de la TI, esto implica evaluar y dirigir la utilización de TI para dar soporte a organizaciones de todo tipo y tamaño, con el fin de conseguir los objetivos planteados, tomando en cuenta políticas

para la monitorización en aspectos de la estrategia para la adecuada utilización de tecnologías de información (Holt & Holt, 2013).

Por tanto, la gobernanza de TI se debe alinear directamente con la estrategia y sus objetivos planteados en relación con la tecnología de la información necesaria en cada uno de los procesos y proyectos establecidos por la organización. Como lo menciona el *IT Governance Institute*, que define un gobierno de TI eficaz como aquel que permite garantizar que TI podrá soportar los objetivos de negocio, optimizar la inversión de negocio en TI y gestionar de forma apropiada los riesgos y oportunidades relacionadas con TI (Georges y Thorp, 2007).

Como se puede apreciar, este es un tema de suma importancia en el desarrollo de este proyecto, principalmente en su alineación con los objetivos del departamento de TI así como de la estrategia organizacional. Gartner también define el gobierno de TI como aquel proceso por el cual se asegura una operación eficaz, eficiente y conforme de la organización de TI (*Definition of IT Governance (ITG) - Gartner Information Technology Glossary*, s. f.).

Con el desarrollo de este proyecto se pretende establecer los aspectos de carácter estratégico y de gestión, con respecto a la seguridad de la información, que permita facilitar a los responsables de la toma de decisiones a lo interno de la organización.

Para lograr esta gobernanza de TI este proyecto se apoya en marcos de referencia y normas internacionales que permitan a las organizaciones definir procesos adecuados en la gestión de la seguridad de la información.

A continuación se describen las normas y marcos de referencia de este proyecto.

2.4. Serie de Normas ISO/IEC 27000

ISO 27000 es un conjunto de estándares creado y gestionado por la *International Organization for Standardization* (ISO) y *la International Electrotechnical Commission* (IEC)

basado en el establecimiento de buenas prácticas con respecto a la implementación, mantenimiento y gestión de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27000 especifica una serie de normas que están relacionadas a la seguridad de la información y su aplicación, las cuales están clasificadas de la siguiente manera:

- Normas que especifican requisitos
    - ISO/IEC 27001 Sistema de gestión de la seguridad de la información
    - ISO/IEC 27006 Requisitos para entidades que auditan y certifican Sistemas de Gestión de la Seguridad de la Información (SGSI).
- Normas que describen guías o directrices generales
    - ISO/IEC 27002 Código de prácticas para los controles de seguridad de la información.
    - ISO/IEC 27003 Guía para la implementación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).
    - ISO/IEC 27004 Gestión de la seguridad de la Información.
    - ISO/IEC 27005 Gestión de riesgos de la seguridad de la Información.
    - ISO/IEC 27007 Guía para la auditoría de los Sistemas de Gestión de la Seguridad de la Información (SGSI).
    - ISO/IEC 27008 Guía para los auditores de controles de la seguridad de la información.
    - ISO/IEC 27014 Gobernanza de la seguridad de la información.
    - ISO/IEC 27016 Gestión de la seguridad de la información.

Además de otras normas que describen guías específicas en la implementación según diferentes sectores de la industria (Blokdyk, 2017).

Los estándares de esta serie de normas que se toman como referencia para el desarrollo de este proyecto son: ISO/IEC 27001 e ISO/IEC 27002, los cuales están enfocados en la seguridad de la información y se especifican a continuación.

2.4.1. ISO 27001:2013 Sistema de Gestión de la Seguridad de la Información

En esta norma se establecen los requisitos para implementar un Sistema de Gestión de Seguridad de la Información en las organizaciones, en esta se definen los objetivos de control que pueden ser seleccionados por las empresas en la creación de su SGSI.

La certificación en esta norma permite a las empresas brindar la confianza a sus clientes en la implementación de controles para preservar la confidencialidad, integridad y disponibilidad de la información y una adecuada gestión su seguridad y riesgos asociados (International Organization for Standardization, 2013).

El presente proyecto se basa en esta norma y permite realizar la verificación de las diferentes áreas y controles en seguridad de la información que muestra el Anexo A de la norma. Además, permite determinar aquellos controles faltantes que son necesarios para mantener su SGSI alineado al estándar y optar por la respectiva certificación.

Para las organizaciones que tomen la decisión estrátegica de implementar un sistema de gestión de la seguridad de la información deberá considerar sus necesidades, objetivos, requerimientos en seguridad de la información, procesos de negocio, tamaño y estructura de forma que el sistema sea adaptado constantemente a través del tiempo (International Organization for Standardization, 2013).

A partir de la aplicación de los diferentes requerimientos establecidos por la norma ISO 27001:2013 la organización podrá mantener una estandarización del proceso de gestión de seguridad de la información que permita la identificación y tratamiento adecuado de los riesgos asociados.

2.4.2. ISO 27002:2013 Código de Prácticas Para los Controles de Seguridad de la Información

Comprende una serie de buenas prácticas y directrices para la correcta implementación de un SGSI. Define la manera en que se pueden cumplir cada uno de los controles especificados por la norma ISO 27001:2013 (International Organization for Standardization, 2013b).

A pesar de que no sea un requisito formal para la certificación en la norma ISO 27001:2013 permite apoyar la implementación y comprensión de los controles que se aplicarán en el SGSI. (Disterer, 2013).

Por esta razón, la presente norma, será de importancia en el desarrollo de este proyecto.

2.5. COBIT 2019

COBIT (*Control Objectives for Information and related Technology*) es un marco de referencia creado por ISACA (*Information Systems Audit and Control Association*) que permite a las empresas mantener una correcta gestión y gobierno de las tecnologías de información alineado a estándares, marcos y regulaciones como lo pueden ser ISO/IEC 27001 e ISO/IEC 27002.

COBIT 2019, en su versión más actualizada, ofrece a las organizaciones la posibilidad de aprovechar las oportunidades que ofrece la tecnología para alinear sus objetivos de TI con la estrategia del negocio, permitiendo un crecimiento y una gestión más eficiente e integral (*COBIT 2019 Framework: Introduction and Methodology*, 2018).

A continuación se especifican los procesos de COBIT enfocados en la seguridad de la información, así como los niveles de capacidad establecidos por este marco de referencia los cuales serán de valor para este proyecto, de acuerdo a la recomendación brindada por la

Auditora CISA, experta consultada en el desarrollo del proyecto (ver Apéndice N. Minutas de Reuniones con la Organización.- Apartado: Tabla N8).

2.5.1. APO13 Gestionar la Seguridad

Este proceso permite definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Su propósito principal es mantener la ocurrencia y el impacto de incidentes relacionados con la seguridad de la información dentro de los niveles aceptables de riesgo establecidos por la empresa (*COBIT*, 2019).

A partir de los siente subprocesos definidos por COBIT (2019) se puede llevar a cabo la verificación de la seguridad de la información de forma que se cuente con un SGSI que cumpla con los objetivos establecidos que permitan controlar los riesgos relacionados con la seguridad de la información, tomando en cuenta las buenas prácticas aplicables que respondan adecuadamente a los recursos organizacionales y marcos normativos.

Este proceso puede aportar prácticas que funcionen como complemento para los controles requeridos de implementar por la organización en el desarrollo del presente proyecto.

2.5.2. DSS05 Gestionar los Servicios de Seguridad

Este proceso se encarga de proteger la información de la empresa de forma que se mantenga dentro de los niveles de riesgo aceptables para la organización especificada en su política interna. Además, establece los roles y privilegios en seguridad y acceso a la información, así como su respectiva supervisión (*COBIT*, 2019).

Según lo establecido por COBIT (2019), el proceso abarca diferentes controles que deben ser tomados en cuenta por organizaciones que busquen minimizar el impacto por vulnerabilidades o incidentes relacionados con la seguridad de la información, de forma que se eviten daños que puedan provocar graves problemas en los procesos de negocio o repercusiones legales para una organización.

De la misma manera que APO13 este será un proceso importante de tomar en cuenta en el desarrollo del proyecto, principalmente en cuanto a los aspectos relacionados con la disponibilidad de los servicios y sistemas que permitan cumplir con las políticas y requerimientos internos de la organización, así como la legislación correspondiente.

2.5.3. Niveles de Capacidad

En cuanto a la calificación de actividades para determinar la capacidad, COBIT (2019) especifica, en la sección “6.4.2 Calificar las Actividades del proceso”, cuatro niveles que permiten evaluar los niveles de porcentaje de cumplimiento como se muestran a continuación.

- **Completamente:** El nivel de capacidad se alcanza para más del 85 por ciento.
- **Largamente:** El nivel de capacidad se alcanza para entre el 50 por ciento y el 85 por ciento.
- **Parcialmente:** El nivel de capacidad se alcanza para entre el 15 por ciento y el 50 por ciento.
- **No:** El nivel de capacidad se alcanza para menos del 15 por ciento.
- Estos niveles serán tomados como referencia para la evaluación de la capacidad en las diferentes áreas que contiene el SGSI desarrollado para este proyecto.

2.6. ITIL Foundation 4 Edition

En ITIL 4 se establecen una serie de buenas prácticas enfocadas en la gestión de áreas técnicas, de servicio y áreas generales en una organización, dentro de ellas se establece un proceso específico en la gestión de la seguridad de la información. Este tiene como propósito proteger toda la información vital para los negocios de la empresa llevando a cabo una correcta gestión de la confidencialidad, integridad y disponibilidad de la información, así como sus riesgos asociados y otros aspectos relacionados con la seguridad de la información como la autenticación y no repudio (*ITIL foundation*, 2019).

2.7. El caso de negocio

El desarrollo de un caso de negocio pretende ofrecer a la organización un respaldo técnico en la inversión financiera de un proyecto, donde se analiza y justifica a través de análisis y estudios los aspectos más relevantes para el éxito del proyecto.

Como lo menciona el ITGI, el objetivo de su documento Val IT es asegurar que las empresas logren conseguir valor de todas sus inversiones bajo un costo adecuado y manteniendo un aceptable nivel de riesgo (Ataya Georges, 2007).

Por esta razón se requiere de un entendimiento claro de la situación actual de la empresa, analizar detalladamente cuál es su entorno en el mercado y determinar las oportunidades que presenta, de forma que se tenga un conocimiento holístico que permita la creación del caso de negocio de acuerdo con su realidad.

Para la creación del caso de negocio en este proyecto se propone implementar lo que establece el documento Val IT que proporciona guías y procesos dirigidos principalmente a las inversiones de negocio correspondientes a TI (Georges & Thorp, 2007). La guía mencionada está compuesta de ocho pasos que se mencionan a continuación.

- Paso 1: Elaboración de una hoja de datos con todos los datos relevantes.
- Paso 2: Análisis de alineación.
- Paso 3: Análisis de beneficios financieros.
- Paso 4: Análisis de beneficios no financieros.
- Paso 5: Análisis de riesgo.
- Paso 6: Evaluación y optimización del riesgo/rendimiento de la inversión posibilitada por TI.
- Paso 7: Registro estructurado de los resultados de los pasos anteriores y documentación del caso de negocio.

- Paso 8: Revisión del caso de negocio durante la ejecución del programa, incluyendo todo el ciclo de vida de los resultados del programa.

Al finalizar con estos pasos se presentará el caso de negocio finalizado como uno de los entregables de este proyecto.

Por otra parte, *COBIT 2019 Framework: Introduction and Methodology* (2018), presenta siete fases para la creación de un caso de negocio que abarcan todo el ciclo de vida del mismo, tomando en cuenta la gestión del programa, la habilitación para cambios y la mejora continua. Estas fases se presentan a continuación.

- Fase 1: ¿Cuáles son los impulsores?
- Fase 2: ¿Dónde estamos?
- Fase 3: ¿Dónde queremos estar?
- Fase 4: ¿Qué debe hacerse?
- Fase 5: ¿Cómo llegamos ahí?
- Fase 6: ¿Lo logramos?
- Fase 7: ¿Cómo mantenemos el impulso?

Para el desarrollo del caso de negocio en este proyecto se pretende adaptar lo expuesto anteriormente para determinar las etapas o fases más adecuadas en relación con el objetivo planteado.

A nivel general, lo que ha sido detallado en este capítulo, respalda las herramientas utilizadas para el desarrollo de este proyecto, de forma que el mismo se encuentre alineado a lo establecido por las organizaciones internacionales.

Capítulo III: Marco Metodológico

En este capítulo se aborda la información referente a la metodología implementada en el desarrollo de este proyecto.

Para contextualizar se toma como referencia el concepto de investigación propuesto por Hernández et al. (2014, p.4) “La investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema”.

En esta sección del trabajo final de graduación se especifican los aspectos relacionados al tipo de investigación y su enfoque, fuentes de información, sujetos de información, categorías de análisis e instrumentos para la recolección de datos. Por último, se definen las diferentes fases realizadas así como la tabla con el resumen del procedimiento metodológico correspondiente a la investigación.

3.1. Tipo de investigación

A pesar del surgimiento de diferentes corrientes de pensamiento a través del tiempo se han establecido tres enfoques principales para una investigación, todos ellos cumplen con la aplicación de los procesos mencionados en la definición anterior, estos modelos son: enfoque cualitativo, enfoque cuantitativo y enfoque mixto (Hernández et al., 2019, p16).

A continuación se especifican los tipos de enfoque cualitativo y cuantitativo, así como el utilizado para el desarrollo de esta investigación en la cual se implementa el enfoque mixto.

3.1.1. Enfoque cualitativo

Al trabajar un enfoque cualitativo se deben plantear diferentes preguntas de investigación e hipótesis a lo largo de su proceso y sus fases, las cuales deben estar siempre apegadas al marco de referencia establecido en la investigación, con el objetivo de resolver las hipótesis que se generan antes, durante o después de la fase de recolección y análisis de datos.

3.1.2. Enfoque cuantitativo

Al realizar una investigación bajo el enfoque cuantitativo se trabaja un modelo secuencial en el que cada etapa precede a la siguiente y se requiere mantener el orden en la ejecución de cada una de ellas.

Este enfoque requiere de una recolección de datos que permitan una medición numérica para probar las hipótesis planteadas.

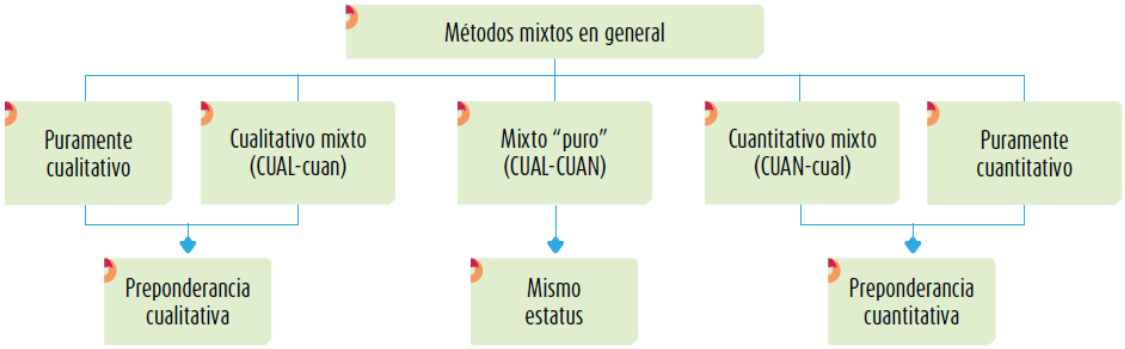
3.1.3. Enfoque mixto

Este modelo de investigación consiste en un conjunto de procesos sistemáticos, empíricos y críticos que requieren de una recopilación y análisis de datos cualitativos y cuantitativos de forma que se logre una integración de los dos enfoques anteriormente mencionados (Hernández et al., 2019).

Como también lo menciona Hernández et al. (2014) en referencia a lo expresado por Chen (2006) el enfoque mixto permite crear un panorama más completo conservando la estructura y los procedimientos originales de los modelos cualitativos y cuantitativos, al mismo tiempo que se realiza una integración sistemática de ambos para lograr un análisis de forma paralela.

Según la categorización de subtipos de estudios mixtos que hace Hernández et al. (2014), para el caso de esta investigación se pretende implementar un método cualitativo mixto el cual contiene una preponderancia cualitativa como se muestra en la figura 4 a continuación.

Figura 4. *Tipos de métodos mixtos*



Fuente: Tomado de Hernández et al. 2014.

3.2. Diseño de la Investigación

Esta etapa es la que permite poner a prueba a través de un plan los resultados preliminares de la investigación, por lo tanto, el diseño de la investigación consiste en una estrategia alineada a los objetivos establecidos la cual permita obtener los datos que respondan a las preguntas planteadas en la hipótesis del problema (Hernández et al., 2014).

Tomando en cuenta que se implementa un enfoque mixto se establece que el diseño de triangulación concurrente (DITRIAC) mencionado por Hernández y Torres (2018) es el modelo que mejor se adapta para esta investigación.

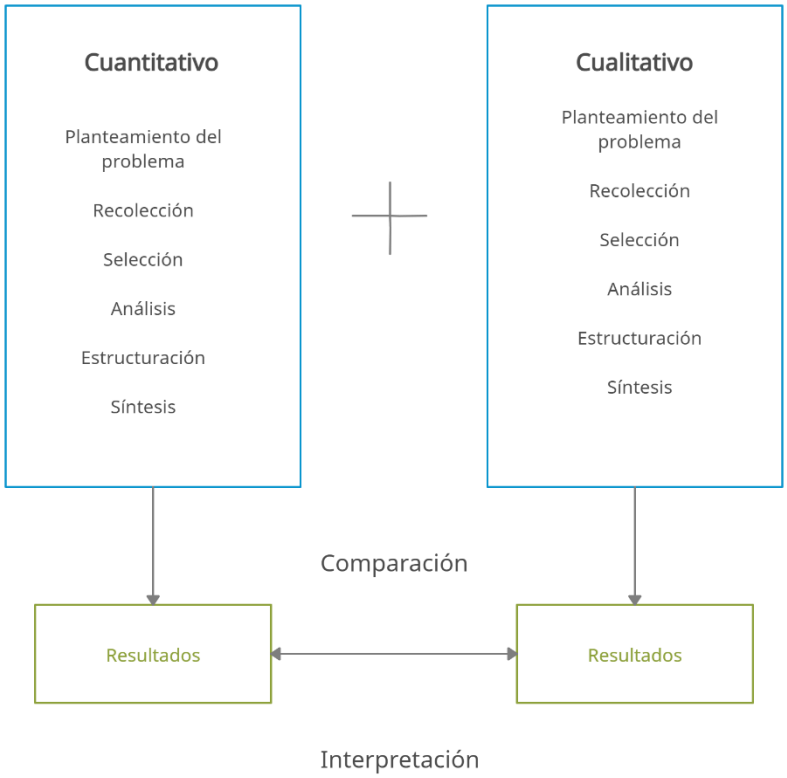
Con el diseño de triangulación se realiza una recolección y análisis de los datos cuantitativos y cualitativos de manera paralela, aprovechando los beneficios de ambos métodos y permitiendo una validación cruzada de los resultados que serán interpretados y comparados entre sí (Hernández y Torres, 2018).

Contemplando lo anterior y lo establecido por la norma ISO/IEC 31010 (2009), la cual define los métodos semicuantitativos como aquellos donde se asignen valoraciones numéricas a partir de la aplicación de alguna fórmula, para el desarrollo de esta investigación se emplea el modelo DITRIAC, el cual permita realizar una evaluación de datos cuantitativos los cuales se

encuentran relacionados a datos cualitativos que requieren de un análisis conjunto de la información.

La siguiente figura 5 muestra una adaptación del modelo realizado por Hernández y Torres (2018).

Figura 5 *Diseño DITRIAC.*



Fuente: Adaptación realizada de Hernández y Torres (2018).

Tomando en cuenta el diseño empleado se aclara que algunos de los instrumentos utilizados se establecerán en el transcurso de la investigación a partir de insumos obtenidos en las fases de Análisis de la situación actual y la fase de Formulación.

3.3. Fuentes de Investigación

Para otorgar el respaldo y la credibilidad a este trabajo se especifican en esta sección las diferentes fuentes de información consultadas.

Según lo mencionado por Razo (2011) se define una clasificación de las fuentes de acuerdo con su origen como se menciona a continuación.

- **Fuentes primarias:** Información obtenida en el mismo punto donde se origina.
- **Fuentes secundarias:** Información obtenida de una interpretación de fuentes primarias.
- **Fuentes terciarias:** Información obtenida de una interpretación de fuentes secundarias.

En esta investigación se recurrió a diferentes fuentes de información las cuales se mencionan en la siguiente tabla 2.

Tabla 3 *Fuentes de investigación*

Fuentes primarias	Fuentes secundarias	Fuentes terciarias
- ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27002 - ISO/IEC 27005 - COBIT 2019 - ITIL 2011 - Políticas internas de la organización (*infosec policy, WIFI internet usage policy, IT change policy, facilities policy, privacy policy*) - Cuestionarios de requerimientos de clientes. - Libros de metodología de investigación (Metodología de La Investigación (6.a ed.), Metodología de la Investigación para	- Bases de datos suscritas del Tecnológico de Costa Rica (AENORmás, Ebooks7-24). - Material académico de la carrera. - Artículo ISACA Val IT. - Trabajos finales de graduación. - Páginas de internet (Gartner, INTERPOL, ESET)	- Clases del curso Formulación y evaluación de proyectos. - Clases del curso Auditoría de TI. - Clases del curso Seguridad de la Información. - Charla *Design thinking.* - Webinar Auditoría de Ciberseguridad.

Fuentes primarias	Fuentes secundarias	Fuentes terciarias
bachillerato (2.a ed.), Cómo Elaborar Y Asesorar Una Investigación De Tesis (2.a ed.). - Expertos en auditoría y seguridad. - Revista Comunicación Empresarial 2007		

3.4. Sujetos de Investigación

En la siguiente tabla 3 se detallan los diferentes sujetos de investigación involucrados en el desarrollo del proyecto.

Tabla 4 *Sujetos de investigación*

Sujeto de Investigación	Años de experiencia	Descripción del Rol	Aporte a la investigación
Asesor de TI	11 años	Encargado de la coordinación de los proyectos y tareas dentro del departamento así como de la toma de decisiones y la administración de adquisiciones. También cuenta con el rol de Jefe de Seguridad por lo que es la persona responsable de mantener la adecuada gestión de la información dentro de la organización.	Visión holística del estado actual de la seguridad de la información en la empresa.

Sujeto de Investigación	Años de experiencia	Descripción del Rol	Aporte a la investigación
Analista de negocio.	3 años.	Analista de negocio encargado de la implementación de cambios en la infraestructura de TI, soporte de tecnologías en la nube y locales. Responsable de la ejecución de la calidad de los procesos operativos y asegurar la continuidad constante del servicio a través del soporte y la gestión de aplicaciones y sistemas comerciales críticos.	Conocimiento detallado de la infraestructura y funciones dentro del departamento, los métodos de gestión implementados y las necesidades de la organización.
Analista de negocio CRM.	2 años.	Analista de negocio CRM encargado de investigar y recopilar datos relacionados con los diferentes clientes de la empresa para generar nuevas estrategias o reportes que permitan fortalecer relaciones y generar nuevas oportunidades de venta.	Conocimiento detallado de las necesidades de los clientes y riesgos críticos de la empresa. Apoyo con conocimientos generales de gestión.
Auditor CISA.	19 años.	Profesora y auditora con conocimientos en COBIT 2019, ITIL y planificación estratégica de TI con certificación CISA *(Certified Information Systems Auditor*).	Amplio conocimiento en la aplicación de auditorías y procesos de certificación de empresas.
Profesores de la carrera.	Variable	Profesores a cargo de cursos como: Administración de procesos de negocio, Formulación y evaluación de proyectos y Seguridad de la Información.	Conocimiento y guía para el desarrollo y ejecución adecuada del proyecto.

3.5. Categorías de la Investigación

Las variables se constituyen por elementos con propiedades fluctuantes en los que se pueden realizar mediciones en las diferentes variantes (Hernández et al., 2014).

Para el desarrollo de esta investigación se emplean diferentes categorías de análisis para alcanzar cada uno de los objetivos específicos planteados.

En la siguiente sección del marco metodológico se especifica en la tabla 4 las diferentes categorías de análisis de esta investigación.

Tabla 5 *Categorías de análisis*

Categoría de análisis	Componentes	Importancia en el proyecto.
Situación actual de la organización en materia de seguridad de la información	Requerimientos de clientes	Cuestionarios de requerimientos obtenidos de diferentes clientes e industrias que contienen las necesidades a ser tomadas en cuenta para la implementación de controles.
	Recursos	Componentes y recursos de la infraestructura de red necesarios para la implementación de controles.
	Limitaciones	Determinar las limitaciones con las que se cuenta para su evaluación y consideración al momento de formular la propuesta.
	Cantidad de actores	Identificar los diferentes actores relevantes para el proyecto.
	Nivel de involucramiento	Involucramiento y relevancia de los actores identificados en el proyecto.
Controles para atacar las brechas según su priorización definida.	Controles	Verificación de los controles de la norma ISO 27001:2013 que están implementados y aquellos que son necesarios de implementar por el departamento de TI.
	Estado Actual	Estado de los controles según la verificación y las observaciones realizadas por parte de los colaboradores del departamento de TI.
	Brechas	Áreas de control en la matriz de evaluación de seguridad de la información que requieren una priorización para su atención de acuerdo con su criticidad.
	Nivel de capacidad	Estado en el que se encuentran los controles verificados según los niveles de capacidad de COBIT.

Requerimientos necesarios para la viabilidad del proyecto	Normativa	Políticas y normas relacionadas con la seguridad de la información.
	Requerimientos legales	Leyes relacionadas con la seguridad de la información.
	Riesgos	Riesgos críticos que pueden comprometer el objetivo del proyecto.
	Indicadores financieros	Determinar la viabilidad económica del proyecto.
	Presupuesto	Recursos financieros disponibles para la implementación de la propuesta.
	Indicadores clave de rendimiento	Métrica para determinar los objetivos de la propuesta.
Actividades requeridas para llevar a cabo la implementación de la propuesta	Estado meta	Determinar las actividades necesarias de llevar a cabo para la futura implementación de la propuesta.
	Matriz RACI	Determinar las actividades necesarias para implementar la propuesta y los responsables de llevarlas a cabo.
	Hojas de verificación	Mantener el seguimiento y control adecuado de la propuesta.
	Recursos	Determinar los recursos humanos y financieros necesarios para implementar la propuesta.

	Tiempo	Estimación del plazo para la implementación de la propuesta y la ejecución de las actividades.

3.6. Instrumentos de Investigación

En una investigación es necesario acudir a los aportes obtenidos desde diferentes fuentes, de forma que se pueda obtener datos que respalden, desde diferentes perspectivas, lo planteado en el proyecto.

Para obtener dichos datos se tienen los instrumentos de investigación, los cuales consisten en los recursos a los que debe acudir el investigador para el registro de la información que permita obtener los resultados de las variables identificadas (Hernández et al., 2014).

En la presente investigación se recurre a utilizar los siguientes instrumentos.

3.6.1. Revisión Documental

Según lo mencionado por Razo (2011) la revisión documental consiste en la recopilación de datos relacionados con la investigación, los cuales provengan de diferentes fuentes, tanto formales como informales, y permitan respaldar dicha información por autores que realizaron una previa investigación.

Para esta investigación se requiere un estudio de los diferentes documentos con las políticas internas de la organización, documentos de requerimientos enviados por los clientes de la organización y documentos de fuentes externas que respalden la propuesta. Posterior al análisis documental la información se sistematiza en la matriz de evaluación de seguridad de la información.

3.6.2. Entrevistas

Para determinar tanto la situación actual como las diferentes etapas posteriores se requiere realizar entrevistas abiertas a los colaboradores del departamento de TI en la organización que permitan identificar aspectos cualitativos por lo que se implementa el tipo de entrevista abierta, de esta forma se pretenden documentar las diferentes observaciones realizadas por los entrevistados (Hernández et al., 2014) (ver Apéndice A. Entrevista con Analista de Negocio de TI. y Apéndice B. Entrevista con Analista de Negocio de CRM.).

3.6.3. Grupo Focal

A través de un grupo focal se pretende profundizar y comprender la perspectiva de diferentes actores de forma que sea posible conocer la interacción entre ellos y obtener una visión completa del problema o tema en cuestión (Hernández et al., 2014) (ver Apéndice C. Grupos Focales.).

3.6.4. Observación

Como lo menciona Hernández et al. (2014) la observación se realiza a través de un método en el que se registre la información y datos de una forma confiable y sistemática donde se registren las diferentes situaciones y comportamientos observables. Tanto para el análisis de la situación actual como para el análisis y documentación de los resultados se requiere utilizar este instrumento de investigación (ver Apéndice D. Verificación del método de observación aplicado.).

Este instrumento será indispensable en la fase de análisis de la situación actual de forma que se obtengan datos reales de los procesos relevantes para el desarrollo del proyecto.

El objetivo principal de la observación es verificar a través de una lista, los controles mencionados por ISO 27001:2013 con respecto a la seguridad de acceso físico, el ambiente

dentro de las operaciones, las actividades, recursos y hechos relevantes para la documentación.

3.6.6. Auditoría de Cumplimiento

Para verificar el estado actual de los controles aplicados por la organización en relación con la gestión de la seguridad de la información que establece ISO 27001:2013 se realiza una auditoría de cumplimiento que permita generar la documentación correspondiente para analizar la situación actual (As-is) y determinar la situación deseada (To-be).De esta forma se podrán establecer las necesidades por resolver.

Como se mencionó anteriormente en este capítulo, el modelo de investigación mixto requiere de un estudio de datos semicualitativos, los cuales se pretenden analizar a través de la matriz “Evaluación de la Seguridad de la Información” obtenida como resultado de la auditoría de cumplimiento aplicada (ver Apéndice H. Matriz de Evaluación de la Seguridad de la Información.).

3.6.7. Análisis de Capacidad

Para realizar el análisis de la capacidad actual de cada una de las áreas de control se toma como criterio de evaluación la siguiente **Tabla 6** Niveles de capacidad COBIT 2019basada en los niveles de capacidad especificados por COBIT 2019.

Tabla 6 *Niveles de capacidad COBIT 2019*

Análisis de capacidad	
Estado	**Descripción**
Completamente	El porcentaje de cumplimiento del área se encuentra en más de un 85%
Largamente	El porcentaje de cumplimiento del área se encuentra entre un 50% y un 85%
Parcialmente	El porcentaje de cumplimiento del área se encuentra entre un 15% y un 50%

Análisis de capacidad	
Estado	**Descripción**
No	El porcentaje de cumplimiento del área se encuentra en menos de un 15%

Fuente: Tomado de COBIT 2019 *Framework: Introduction and Methodology*.

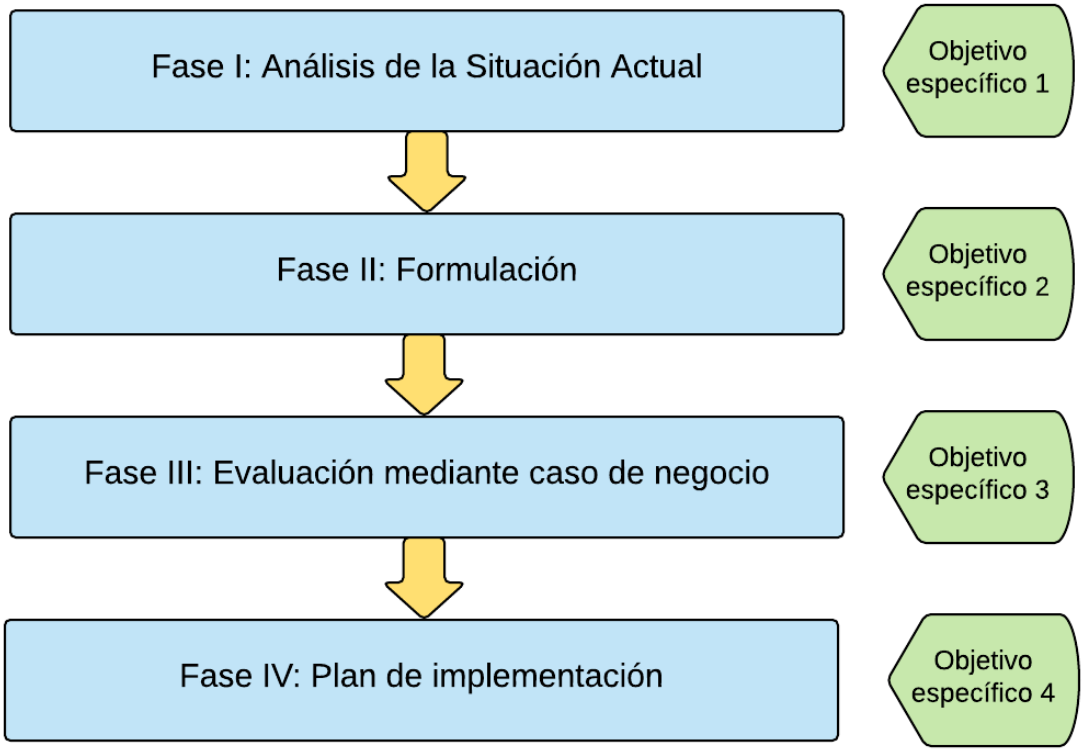
Tomando como referencia los niveles mencionados se pretende establecer la debida priorización de las áreas que requieran atención según el porcentaje de cumplimiento de los controles verificados en la auditoría de cumplimiento.

3.7. Procedimiento Metodológico de la Investigación

En esta sección se pretende detallar el procedimiento metodológico empleado, en el cual se incluyen las diferentes fases que comprende el desarrollo del presente proyecto.

Para el procedimiento se definen cuatro fases las cuales responden a los objetivos específicos planteados como se muestra en la figura 6 y posteriormente se detalla cada una de las fases.

Figura 6 Procedimiento metodológico



3.7.1. Fase I: Análisis de la Situación Actual

Como primer paso para el desarrollo de este proyecto se requiere tener el contexto de la organización, para esto se realiza un análisis de la situación actual en Mobilize.NET que permite conocer trabajos realizados previamente en la organización, de forma que el proyecto llegue a complementar con todo lo necesario para obtener la certificación.

Para conseguir esto se emplea el uso de diferentes instrumentos de investigación que permitan llevar a cabo las tareas que se mencionan a continuación.

- **Revisión documental:** Se analizaron los siguientes documentos que permitieron establecer el contexto y herramientas necesarias.
    - Políticas internas de la organización.
    - Cuestionarios con requerimientos de clientes.
    - Normas ISO 27001:2013 e ISO 27002:2013.

- **Entrevista:** Se realizan entrevistas abiertas para conocer el contexto de la situación actual de la seguridad de la información y comprender la raíz del problema que se pretende solventar.
    - Entrevista con analista de negocio.
    - Entrevista con analista de negocio CRM.
- **Marco lógico:** Se emplea la aplicación del marco lógico hasta su fase de formulación que brinden el panorama de las necesidades a resolver.
    - Identificación de los involucrados del proyecto.
    - Árbol de problemas.
    - Árbol de objetivos (ver Apéndice L. Árbol de Objetivos.)

Al conocer en qué punto se encuentra la organización y sabiendo los requerimientos necesarios para la certificación, se procede con la siguiente fase del proyecto.

3.7.2. Fase II: Formulación

Una vez se tenga el contexto de la organización se plantea, como siguiente paso, realizar la investigación necesaria en torno a la seguridad de la información, específicamente en la norma ISO 27001:2013, donde se pretende mapear los criterios faltantes para definir las acciones a realizar que permitan el alineamiento de los procesos de la empresa con los requerimientos necesarios para la certificación.

Además se identifican las principales preocupaciones de los clientes en materia de seguridad de la información con el fin de atacar estas necesidades con la propuesta que se pretende plantear.

Para llevar a cabo las tareas necesarias en esta fase se recurre a los siguientes instrumentos de investigación.

- **Revisión documental:** Para esta fase se requiere profundizar en algunos documentos consultados en la fase anterior, así como reforzar los conocimientos para la formulación de la propuesta.
    - Cuestionarios con requerimientos de clientes.
    - Normas ISO 27001 e ISO 27002.
    - Niveles de capacidad COBIT 2019.
- **Entrevista:** Se realizan diferentes reuniones para verificar la formulación de la matriz de evaluación de seguridad de la información.
    - Entrevista abierta con Analista de Negocio de TI (ver Apéndice A. Entrevista con Analista de Negocio de TI.).
    - Entrevista abierta con Analista de Negocio CRM (ver Apéndice B. Entrevista con Analista de Negocio de CRM.).

  Los resultados de dichas entrevistas se pueden consultar en el Apéndice N. Minutas de Reuniones con la Organización. en los apartados Tabla N1 y Tabla N2.
- **Grupo focal:** Se organizará un grupo focal para determinar el estado actual y las fórmulas para el cálculo del cumplimiento por área de control, así como los factores críticos de éxito del proyecto.
    - Grupo focal con analista de negocio y analista de negocio CRM (ver Apéndice C. Grupos Focales. – Apartado: Tabla C1).
    - Grupo focal con el asesor de TI, analista de negocio y analista de negocio CRM (ver Apéndice C. Grupos Focales.– Apartado: Tabla C2).
- **Auditoría:** Se realiza una auditoría de cumplimiento a través de las entrevistas mencionadas para la verificación de los diferentes controles incluidos en la

matriz de evaluación de seguridad de la información en relación con los objetivos mencionados en la norma ISO 27002:2013.

3.7.3. Fase III: Evaluación Mediante el Caso de Negocio

En esta fase se realizan los diferentes estudios y análisis que permitan respaldar la propuesta desde una perspectiva técnica y financiera, de forma que se logre establecer el caso de negocio que determine la viabilidad del proyecto.

Los estudios que se establecen para el proyecto son:

- Estudio Técnico.
- Estudio de Mercado.
- Análisis de Riesgos.
- Estudio Financiero.

Los resultados obtenidos a través de dichos estudios serán el insumo requerido para definir el documento del caso de negocio de forma que se abarquen todos los aspectos que la organización debe analizar con respecto a la propuesta.

3.7.4. Fase V: Plan de Implementación

Por último, se define la fase que comprende el plan de implementación, el cual contiene las actividades, responsables y cronograma a seguir en la futura ejecución del caso de negocio planteado en la fase anterior.

Para definir la propuesta de implementación se requiere establecer una matriz de asignación de responsabilidades, donde se especifique el nivel de responsabilidad de cada colaborador en la ejecución de la propuesta.

Por último se establecen las hojas de verificación como instrumento correspondiente al adecuado control que permita recabar los datos sistemáticamente de forma que se puedan establecer las correcciones y mejoras de la propuesta.

3.8. Tabla Resumen del Procedimiento Metodológico de la Investigación

En esta sección se resume, mediante la **Tabla 7**, las anteriores secciones de este capítulo de forma que se logre una conceptualización y alineación con los objetivos específicos del proyecto.

A continuación se muestra cada uno de los objetivos específicos de la investigación con su respectiva categoría de análisis y conceptualización, así como los instrumentos e indicadores que fueron utilizados para llevar a cabo dichos objetivos.

Tabla 7 *Resumen metodológico.*

Fase	Objetivo específico	Conceptualización de la categoría de análisis	Indicadores	Instrumentos
1.	Analizar la situación actual de la empresa para la identificación de los controles en seguridad de la información necesarios y el cumplimiento de los requerimientos recibidos.	Priorización de las brechas a contemplar en la propuesta considerando las necesidades de los clientes y la capacidad de la empresa.	- Controles actuales. - Requerimientos. - Necesidades de clientes. - Nivel de madurez en gestión de seguridad de la información. - Requerimientos en materia de seguridad de información según enfoque ISO 27001.	• Revisión documental. • Entrevistas. • Grupo focal.
2.	Establecer los aspectos estratégicos, técnicos y de gestión necesarios para atacar las brechas identificadas.	Determinar los controles para atacar las brechas identificadas.	- Cantidad de actores. - Nivel de involucramiento de actores. - Limitaciones. - Controles necesarios.	• Investigación documental familia ISO 27000 Seguridad de la Información. • Análisis documento "Evaluación de Seguridad de la Información" • Análisis matricial de cuestionarios de requerimientos de clientes. • Árbol de objetivo. • Identificación de actores.
3.	Desarrollar los estudios de factibilidad necesarios que permitan determinar la viabilidad de la certificación.	Establecer los requerimientos necesarios para la viabilidad del proyecto.	- Normativa y requerimientos legales. - Riesgos críticos. - Indicadores financieros.	• Estudio Técnico. • Estudio de Mercado. • Análisis de riesgos. • Análisis financiero.

Fase	Objetivo específico	Conceptualización de la categoría de análisis	Indicadores	Instrumentos
4.	Elaborar una propuesta de implementación que brinde la guía necesaria para obtener la Certificación en ISO 27001:2013 para el departamento de TI en la empresa.	Determinar las actividades requeridas para llevar a cabo la implementación de la propuesta.	- Indicadores clave de rendimiento. - Resultado de hojas de verificación. - Presupuesto del departamento. - Estimación de tiempo. - Cantidad de actividades.	• Definición de objetivos e indicadores clave de rendimiento. • Cronograma. • Tabla RACI. • Recursos. • Hojas de verificación.

3.9. Matriz de Trazabilidad

En la siguiente **Tabla 8** se muestran los instrumentos de investigación requeridos para cada una de las categorías de análisis planteadas en el presente proyecto de forma que se identifique el grado de cobertura que tendrán dichos instrumentos en cada una de las categorías como se muestra a continuación.

Tabla 8 *Matriz de Trazabilidad.*

Categoría de Análisis	Entrevistas	Grupo Focal	Observación	Revisión Documental	Auditoría	Marco Lógico
Priorización de las brechas a contemplar en la propuesta considerando las necesidades de los clientes y la capacidad de la empresa.	X		X	X		X
Determinar los controles para atacar las brechas identificadas.	X	X	X	X	X	
Establecer los requerimientos necesarios para la viabilidad del proyecto.	X	X		X		
Determinar las actividades requeridas para llevar a cabo la implementación de la propuesta.	X			X		

Capítulo IV: Análisis de Resultados

En este capítulo se presentan los resultados obtenidos a partir de la aplicación de los instrumentos de investigación detallados previamente para cada una de las fases del proyecto.

Para realizar el análisis de los datos se toma como referencia lo expresado por Razo (2011) el cual menciona que este proceso consiste en realizar una “agrupación de datos en rangos significativos que se concentran conforme a una adecuada selección para dar una interpretación útil al investigador”.

A continuación se detallan los resultados obtenidos en el desarrollo del proyecto, los cuales serán el fundamento principal en el cumplimiento de los objetivos planteados.

4.1. Análisis de la Situación Actual

Para la primera etapa del proyecto fue necesaria una contextualización a través de la aplicación de diferentes instrumentos de investigación mencionados en la sección

3.6. Instrumentos de Investigación del presente documento.

Mediante los instrumentos de revisión documental, entrevistas, grupo focal y observación se obtuvo como resultado la matriz “Evaluación de la Seguridad de la Información” (ver Apéndice I). A continuación se detallan las diferentes secciones que lo componen así como los resultados obtenidos.

4.1.1. Áreas de Seguridad de la Información.

Para definir las áreas de control en seguridad de la información y lograr una correcta alineación en el proyecto se recurre a una revisión de los principales documentos que fueron el principal insumo para definir la estructura de la matriz mencionada.

Primeramente, se establecen los controles que fueron tomados en cuenta para conformar la plantilla para la matriz de evaluación, los cuales son los especificados por la

norma ISO 27001:2013 en su anexo A “Objetivos de control y controles de referencia” conformado por catorce áreas de control que se mencionan a continuación.

1. Políticas de seguridad de la información.
2. Organización de seguridad de la información
3. Seguridad ligada a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del ambiente.
8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de los sistemas de información.
11. Relaciones con los proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
14. Cumplimiento.

Para la creación de la herramienta se incluyen todas las áreas mencionadas con cada uno de los controles correspondientes, los cuales suman en total 144, de forma que el documento sea de valor en caso de optar por la certificación correspondiente a la norma.

A partir del análisis realizado a los cuestionarios de requerimientos enviados por los clientes de la empresa, se determina que las necesidades expresadas con respecto a la seguridad de la información se encuentran relacionados en los controles que establece la norma ISO 27001:2013. Además, en la reunión con el equipo de trabajo, se identifican cuatro áreas de control importantes de tomar en cuenta para ser agregadas y lograr un alineamiento

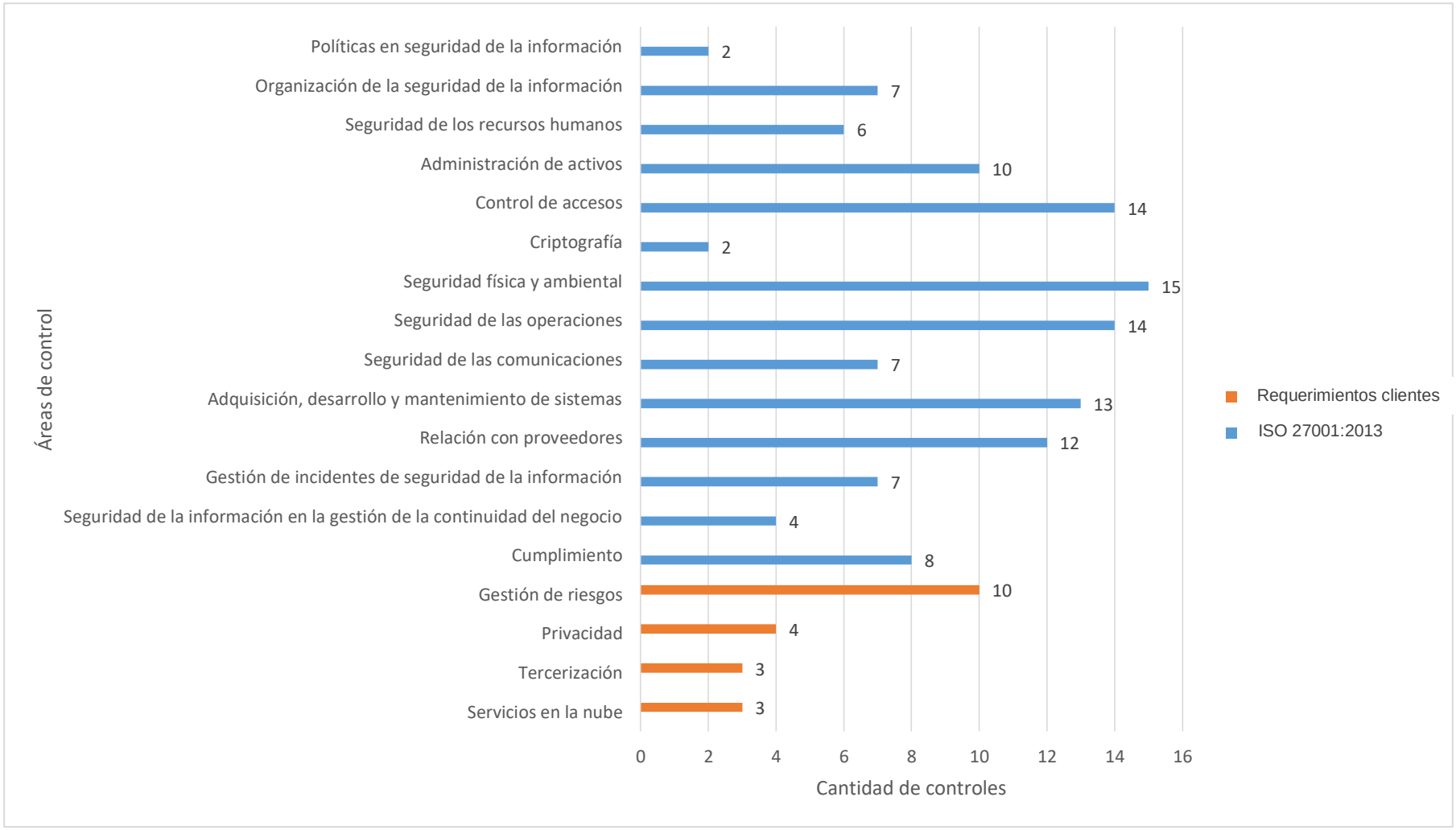
de la herramienta con la industria (ver Apéndice N. Minutas de Reuniones con la Organización.- Apartado: Tabla N14).

15. Gestión de riesgos.
16. Privacidad.
17. Tercerización.
18. Servicios en la nube.

Producto de este análisis de clientes se agregaron, a estas cuatro áreas, un total de veinte controles que corresponden a requerimientos encontrados en los cuestionarios enviados por clientes y que formarán parte de la matriz de evaluación.

A continuación se muestra la **Figura 7** que contiene un resumen gráfico de las 18 áreas y los 164 controles establecidos para definir la herramienta. Además, se identifican las áreas tomadas de la norma ISO 27001:2013 y las áreas tomadas de los requerimientos de clientes.

Figura 7 *Cantidad de controles por área*



Estas áreas y controles fueron verificadas mediante reuniones, en las que participaron la Analista de Negocio de TI y el Analista de Negocio CRM del Departamento de TI (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N4).

4.1.2. Auditoría de Cumplimiento

Con la aplicación de una auditoría de cumplimiento se pretende definir cuáles controles se tienen debidamente implementados y cuáles controles no se cumplen, además de aquellos que, por naturaleza del negocio o por políticas internas, no apliquen para ser evaluados.

Para la verificación del nivel de cumplimiento de cada una de las áreas de control se define, en conjunto con los colaboradores del departamento de TI, un estado actual con su respectiva calificación e identificación para cada uno de los controles. En la siguiente **Tabla 9** se muestra el criterio de evaluación establecido.

Tabla 9 *Estado Actual*

Estado Actual	Descripción
3	Se aplican las acciones adecuadas y se cumple con los requerimientos en el control.
2	Se realizan algunas acciones pero existen oportunidades de mejora o necesidades para cumplir con los requerimientos en el control.
1	No se aplican las acciones requeridas para cumplir con los requerimientos en el control.
N/A	El control no aplica de acuerdo con las políticas de la organización.

Fuente: Apéndice N. Minutas de Reuniones con la Organización., Tabla N10. Reunión con colaboradores del Departamento de TI.

Para realizar la auditoría de cumplimiento fueron necesarias reuniones virtuales con los colaboradores del departamento en la que se aplicaron las entrevistas abiertas mencionadas en la sección 3.7.2. Fase II: Formulación para la verificación basada en la norma ISO 27002:2013.

A continuación se muestran los resultados obtenidos en cada una de las áreas y sus controles posterior a las observaciones obtenidas y la definición de su estado actual.

4.1.2.1. Políticas de Seguridad de la Información. Como se muestra en la **Tabla 10** esta área cuenta únicamente con dos controles.

Tabla 10 Políticas de Seguridad de la Información

Controles	Sí	No	N/A	Estado actual
Políticas para la seguridad de la información	X			**3**
Revisión de las políticas para la seguridad de la información	X			**3**

El primer control corresponde con las políticas para la seguridad de la información, las cuales se encuentran debidamente documentadas, aprobadas y comunicadas a los empleados y partes externas relevantes, por lo que obtiene la puntuación máxima en su estado actual.

En su segundo control se verifica la revisión de las políticas en seguridad de la información la cual se realiza de manera periódica por los responsables debidamente asignados, así como las correspondientes actualizaciones a la política, por lo que también define su estado actual máximo.

Contar con todos los controles debidamente implementados de acuerdo con lo mencionado por la International Organization for Standardization (2013b), permite a la empresa

proporcionar una adecuada orientación y apoyo hacia la gestión de la seguridad de la información, alineando aspectos legales y normativos con los requerimientos del negocio en su documentación de políticas.

4.1.2.2. Organización de Seguridad de la Información. En la **Tabla 11** se muestran los controles del área y su respectivo estado actual.

Tabla 11 *Organización de la Seguridad de la Información*

Controles	Sí	No	N/A	Estado actual
Roles y responsabilidades en seguridad de la información	x			**3**
Segregación de deberes	x			**3**
Contacto con las autoridades		x		**1**
Contacto con grupos de interés especiales	x			**2**
Seguridad de la información en la administración de proyectos	x			**3**
Política de dispositivos móviles	x			**2**
Teletrabajo	x			**3**

En esta área la organización cuenta con los roles y responsabilidades debidamente establecidos y asignados con respecto a la seguridad de la información y el manejo de aspectos como accesos, activos y clientes. Además se cuenta con una adecuada segregación de deberes entre los responsables para mantener la seguridad y el acceso limitado.

Para mantener la seguridad en la administración de los proyectos se mantiene como único responsable de asignar los recursos y permisos de acceso al administrador del proyecto.

El último control que se encuentra en su cumplimento total es la política de teletrabajo, la cual se mantiene un documento debidamente establecido, aprobado y comunicado a todos los departamentos y colaboradores de la organización.

Estos controles que se encuentran implementados permiten a la organización establecer los principales aspectos para controlar la implementación y operación de la seguridad de la información a través de un adecuado marco de gestión (International Organization for Standardization, 2013b).

Para el contacto con grupos de interés se define una calificación media para su estado actual, ya que cuentan con notificaciones correspondientes a actualizaciones o cambios relacionados a los sistemas utilizados por la empresa, sin embargo se tienen oportunidades de mejora para aumentar la cobertura a más sistemas relevantes de manera que esto brinde una mayor cooperación y coordinación en el intercambio de información relevante para la seguridad de la información.

De la misma forma, la política de dispositivos móviles cuenta con controles enfocados en la seguridad de dispositivos organizacionales pero se requiere de una política BYOD (*Bring Your Own Device*), la cual tenga como objetivo brindar la seguridad necesaria en el uso de dispositivos móviles y su riesgo de acceso no autorizado, de forma que no se comprometa en ningún momento la información del negocio.

En el caso del control correspondiente al contacto con las autoridades respectivas el departamento carece de documentación donde se establezcan los procedimientos correspondientes para los casos en los que se requiera informar a alguna autoridad sobre posibles incidentes. A pesar de que los colaboradores del departamento conocen la importancia de realizar los contactos con las autoridades correspondientes en una situación determinada, se establece que este control no se tiene debidamente implementado, lo que

puede provocar la ejecución indebida del proceso por otros colaboradores o incluso que no se realice del todo por la falta de conocimiento del mismo.

4.1.2.3. Seguridad Ligada a los Recursos Humanos. Como se puede observar en la **Tabla 12**, en esta área se tienen dos controles con una calificación media en su estado actual debido a que presentan oportunidades de mejora.

Tabla 12 *Seguridad Ligada a los Recursos Humanos*

Controles	Sí	No	N/A	Estado actual
Proyección	x			**3**
Términos y condiciones del empleo	x			**3**
Administración de responsabilidades	x			**3**
Concientización, educación y capacitación en seguridad de la información	x			**2**
Proceso disciplinario	x			**2**
Finalización o cambio de responsabilidades laborales	x			**3**

El primero de estos controles corresponde con la concientización, educación y capacitación en seguridad de la información, en el cual se le brinda información general a cada colaborador al momento de ingresar a la organización, sin embargo, la concientización y capacitación se encuentran en proceso de implementación. Tomar estas oportunidades de mejora brinda a los colaboradores de la organización un pensamiento crítico que permita estar atentos a las preocupaciones en seguridad de la información que corresponden a su puesto.

En cuanto al proceso disciplinario se mantiene un proceso con pasos definidos pero es necesario realizar su respectiva documentación con el objetivo de formalizar el proceso y dar a

conocer a todos los colaboradores las acciones disciplinarias a las que se exponen en caso de generar alguna brecha de seguridad. También pueden incluirse recompensas o incentivos que motiven los comportamientos notables para garantizar la seguridad de la información.

Para los demás controles del área se logró verificar su correcta implementación y cumplimiento obteniendo la calificación máxima en su estado actual. Esto permite mantener a los diferentes empleados y personas subcontratistas al tanto de las responsabilidades que asumen de acuerdo a sus funciones como lo establece la International Organization for Standardization (2013b).

4.1.2.4. Gestión de Activos. En la siguiente **Tabla 13** se muestran los resultados en el área de gestión de activos.

Tabla 13 *Gestión de Activos*

Controles	Sí	No	N/A	Estado actual
Inventario de activos	x			**3**
Propiedad de los activos	x			**3**
Uso adecuado de los activos	x			**2**
Devolución de los activos	x			**2**
Clasificación de la información		x		**1**
Etiquetado de información		x		**1**
Manejo de los activos	x			**3**
Gestión de medios extraíbles		x		**1**

Controles	Sí	No	N/A	Estado actual
Eliminación de los medios		x		1
Transporte de medios físicos		x		1

Como se observa, la empresa cuenta con los respectivos controles en la seguridad de sus activos, donde se mantiene un inventario debidamente identificado, registrado, almacenado y actualizado, también se mantienen procesos para su debida gestión. Así mismo se designa como propietario a cada uno de los colaboradores que estén a cargo de la utilización de un activo. Por esta razón se asigna la calificación máxima en los primeros dos controles del área.

De la misma forma se verifican los controles con respecto al manejo de los activos los cuales se mantienen debidamente identificados bajo etiqueta física y se gestionan a través de la mesa de servicio, obteniendo su estado actual máximo para este control.

Estos controles implementados permiten al departamento mantener un avance importante en la correcta identificación de los activos de la organización y los responsables de su adecuado mantenimiento (International Organization for Standardization, 2013b).

En cuanto al uso adecuado de los activos, la empresa no presenta un proceso documentado formalmente, el mismo se encuentra en desarrollo. Actualmente se tiene definido y próximamente se realizará la comunicación a las partes correspondientes.

De la misma manera se implementa un proceso para la devolución de los activos donde se realiza el formateo de la información contenida en el dispositivo previo a su entrega, sin embargo se requiere de su debida documentación.

Por esta razón se define un estado actual con calificación media para estos dos controles mencionados anteriormente. Al atender las oportunidades de mejora se espera que se logre generar una mayor conciencia en el uso de activos que genere una mayor responsabilidad sobre los recursos de tratamiento de la información, así como una mayor documentación de los procesos que establezcan las acciones establecidas en la correcta gestión de los activos.

La organización carece de controles para el etiquetado y clasificación de la información, además de la gestión, eliminación y transporte de medios. Debido a la falta de implementación de estos controles se define una calificación mínima en su respectivo estado actual.

La ausencia de dichos controles genera brechas de seguridad en la organización donde se pueden presentar vulnerabilidades importantes de tomar en cuenta para gestionar adecuadamente los riesgos asociados.

4.1.2.5. Control de Acceso. La **Tabla 14** correspondiente al área de control de acceso muestra los siguientes resultados.

Tabla 14 *Control de Acceso*

Controles	Sí	No	N/A	Estado actual
Política de control de accesos	x			**2**
Acceso a redes y servicios de red	x			**3**
Registro y deshabilitación de usuarios	x			**3**
Aprovisionamiento de acceso a usuarios	x			**3**
Gestión de derechos de acceso privilegiado	x			**3**

Controles	Sí	No	N/A	Estado actual
Gestión de la información secreta de autenticación de usuarios	x			**3**
Revisión de los derechos de acceso de los usuarios		X		1
Eliminación y ajustes de los derechos de acceso	x			**3**
Uso de la información secreta de autenticación de usuarios	x			**3**
Restricciones de acceso a la información	x			**3**
Procedimientos de inicio de sesión seguros	x			**3**
Sistema de gestión de contraseñas	x			**3**
Uso privilegiado de los programas de utilidad	x			**3**
Control de acceso a código fuente de programas	x			**3**

Con respecto a la política de control de accesos se verifica que, a pesar que se cuentan con controles implementados, los mismos requieren ser reforzados y documentados, definiéndose un estado actual con calificación media.

El único control que se identifica con un estado actual mínimo corresponde con la ausencia de revisiones de los derechos de acceso de los usuarios.

Para los demás controles del área se verifica el cumplimiento adecuado, por lo que se otorga la calificación máxima en su estado actual.

Atender las oportunidades de mejora e implementar adecuadamente los controles que permitan el cumplimiento total de esta área es de gran valor para el departamento en la

adecuada gestión de los recursos de información y la protección contra accesos no autorizados según lo establece la International Organization for Standardization, (2013b).

4.1.2.6. Criptografía. Para el área de criptografía se tienen dos controles, en ambos se define un estado actual medio como se muestra en la **Tabla 15**.

Tabla 15 *Criptografía*

Controles	Sí	No	N/A	Estado actual
Políticas en el uso de controles criptográficos	x			**2**
Gestión de claves	x			**2**

En cuanto a las políticas en controles criptográficos la empresa cuenta con controles para la encriptación del disco duro únicamente en laptops y no se realiza de la misma manera para las computadoras de escritorio y servidores, los cuales se encuentran pendientes de implementar.

En el caso de la gestión de claves, estas se generan adecuadamente mediante la herramienta de Microsoft BitLocker, sin embargo son almacenadas en archivos de Excel, generando riesgos y presentando oportunidades de mejora.

Como lo establece la International Organization for Standardization, (2013b), implementar las mejoras correspondientes en los controles criptográficos permite garantizar la protección y aseguramiento de la confidencialidad, autenticidad e integridad de la información.

4.1.2.7. Seguridad Física y del Ambiente. En la siguiente **Tabla 16** se muestran los controles del área y su respectivo estado actual.

Tabla 16 *Seguridad Física y del Ambiente.*

Controles	Sí	No	N/A	Estado actual
Perímetro físico de seguridad	x			**3**
Controles de ingreso físicos	x			**3**
Aseguramiento de oficinas, salas e instalaciones.	x			**3**
Protección contra amenazas externas y ambientales	x			**3**
Trabajo en áreas seguras	x			**3**
Áreas de carga y entrega	x			**3**
Ubicación y protección del equipo	x			**3**
Instalaciones de suministro	x			**3**
Seguridad del cableado	x			**3**
Mantenimiento del equipo	x			**2**
Retiro de activos	x			**3**
Seguridad de equipo y activos fuera de las instalaciones	x			**3**
Eliminación o reutilización segura de equipos	x			**3**
Equipo de usuario desocupado	x			**3**
Política de escritorio y pantalla limpios	x			**3**

Como se observa en esta área de control únicamente se presentan oportunidades de mejora en cuanto al mantenimiento de los equipos. Este mantenimiento se realiza por el encargado responsable del activo, sin embargo deben implementarse controles para la verificación.

En el caso de los demás controles correspondientes al área de seguridad física y ambiental, se verificó el adecuado cumplimiento a través de reuniones con los colaboradores del Departamento de TI (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N4). Además se realiza una visita a las oficinas de la organización para aplicar el instrumento de observación, mencionado en la sección

3.6. Instrumentos de Investigación de este documento el cual se evidencia en el Apéndice D. Verificación del método de observación aplicado.

Contar con los controles establecidos por el área de “Seguridad física y ambiental” genera la prevención requerida para prevenir accesos no autorizados, además de la interferencia o daños que puedan ser provocados a la información o activos como lo menciona el objetivo de la International Organization for Standardization (2013b).

4.1.2.8. Seguridad de las Operaciones. Al observar los resultados de la **Tabla 17** se determina que existen brechas por atender únicamente en dos controles.

Tabla 17 *Seguridad de las Operaciones.*

Controles	Sí	No	N/A	Estado actual
Documentación de procedimientos operativos	x			**3**
Gestión del cambio	x			**3**
Gestión de la capacidad	x			**3**
Separación entre entornos de desarrollo, pruebas y operativos	x			**3**
Controles contra malware	x			**3**
Respaldos y copias de seguridad de la información	x			**3**

Controles	Sí	No	N/A	Estado actual
Registro de eventos	x			**3**
Protección de la información de registro	x			**3**
Registros de administrador y operador	x			**3**
Sincronización de tiempo	x			**3**
Instalación de software en sistemas operativos	x			**3**
Gestión de vulnerabilidades técnicas	x			**3**
Restricciones en la instalación de software	x			**2**
Controles de auditoría en sistemas de información		x		**1**

El primero de los controles que requiere atención corresponde con las restricciones para la instalación de software. A pesar que el departamento cuenta con restricciones establecidas para el uso de programas que tienen alto consumo de banda ancha, la instalación y uso de los mismos es controlada únicamente cuando se perciben impactos en la red, de modo que cumplir con estas restricciones se encuentra bajo responsabilidad de cada colaborador.

Mantener estas restricciones debidamente controladas reduce la posibilidad que se introduzcan vulnerabilidades que afecten las operaciones y la seguridad de la información.

En cuanto a las auditorías internas a los sistemas de información se requiere la implementación del proceso adecuado que permita la supervisión y comprobación de los riesgos asociados a las operaciones del negocio.

4.1.2.9. Seguridad de las Comunicaciones. Para el área de seguridad se requieren acciones únicamente en la segregación de redes como se muestra en la **Tabla 18**.

Tabla 18 *Seguridad de las Comunicaciones.*

Controles	Sí	No	N/A	Estado actual
Controles de red	x			**3**
Seguridad de los servicios de red	x			**3**
Segregación en redes		x		**1**
Políticas y procedimientos para la transferencia de información	x			**3**
Acuerdos sobre la transferencia de información	x			**3**
Mensajería electrónica	x			**3**
Acuerdos de confidencialidad y no divulgación	x			**3**

La carencia de dicho control provoca riesgos al compartir recursos de red, existiendo vulnerabilidades en el acceso no autorizado a sistemas y la transferencia, tanto interna como externa, de información sensible o de carácter crítico para la organización.

En el resto de controles que pertenecen al área se verifica un adecuado cumplimiento e implementación, lo cual brinda una debida protección de las redes al y los recursos para el tratamiento de la información según lo establece la International Organization for Standardization (2013b).

4.1.2.10. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

En la siguiente **Tabla 19** se muestra el estado actual de los controles correspondientes al área de adquisición, desarrollo y mantenimiento de los sistemas de información.

Tabla 19 *Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.*

Controles	Sí	No	N/A	Estado actual
Análisis y especificación de requerimientos en seguridad de la información	x			**3**
Protección de los servicios de aplicaciones en redes públicas	x			**3**
Protección de transacciones en servicios de aplicaciones	x			**3**
Política de desarrollo seguro	x			**3**
Procedimientos de control de cambios del sistema	x			**3**
Revisión técnica de aplicaciones después de cambios de plataforma operativa	x			**3**
Restricciones sobre cambios en paquetes de software	x			**3**
Principios de ingeniería de sistemas seguros	x			**3**
Entorno de desarrollo seguro	x			**3**
Desarrollo subcontratado	x			**3**
Pruebas de seguridad del sistema	x			**3**
Pruebas de aceptación del sistema	x			**3**
Protección de los datos de prueba	x			**3**

En la verificación que se muestra en la **Tabla 19** se puede observar que la organización cuenta con controles debidamente establecidos en el ciclo de vida de los procesos de

migración y los diferentes sistemas de información, de forma que se garantice el objetivo que define la International Organization for Standardization (2013b), en la integración con los aspectos en seguridad de la información para la protección de datos.

4.1.2.11. Relaciones con los Proveedores. La **Tabla 20** ilustra los controles correspondientes con la gestión de la relación con proveedores los cuales se analizan a continuación.

Tabla 20. *Relaciones con los Proveedores.*

Controles	Sí	No	N/A	Estado actual
Política de seguridad de la información para las relaciones con proveedores		x		**1**
Abordar la seguridad dentro de los acuerdos con proveedores	x			**3**
Cadena de suministro de las tecnologías de información y comunicación		x		**1**
Control y revisión de los servicios de proveedores	x			**3**
Gestión de cambios en los servicios de proveedores		x		**1**

Se identifica el cumplimiento en cuanto a los requerimientos de seguridad dentro de los acuerdos con proveedores, los cuales se encuentran documentados a través de las respectivas políticas de privacidad al momento de adquirir las licencias.

También se realizan las revisiones a los servicios correspondientes en donde se mantienen reuniones mensuales con proveedores locales. En cuanto a proveedores externos y servicios a través de licencias se realizan revisiones de los recursos y servicios en uso para su

reporte o actualización al proveedor, además se reciben actualizaciones para evaluar que se mantenga la seguridad de la información.

Con la implementación de los anteriores controles la organización establece las primeras acciones para asegurar la protección de los activos que requieran el acceso de proveedores.

Sin embargo, se encuentran brechas importantes al no contar con una política establecida, tampoco se tienen procesos definidos para la gestión de la cadena de suministro y la gestión de cambios en los servicios con proveedores.

A pesar que se evalúan los riesgos en los diferentes contratos, es importante tomar en cuenta lo establecido por la International Organization for Standardization (2013b) para generar la documentación pertinente a la relación con los proveedores y sus procesos, de forma que se tengan claras las acciones y controles para todos los responsables.

4.1.2.12. Gestión de Incidentes de Seguridad de la Información. La organización cuenta con acciones implementadas para los controles correspondientes a la gestión de los incidentes de seguridad de la información, la mayoría de estos controles se encuentran implementados en su totalidad como se muestra en la **Tabla 21**.

Tabla 21. *Gestión de Incidentes de Seguridad de la Información.*

Controles	Sí	No	N/A	Estado actual
Responsabilidades y procedimientos	x			**3**
Informe de eventos en seguridad de la información	x			**3**
Informe de debilidades en seguridad de la información	x			**3**

Controles	Sí	No	N/A	Estado actual
Evaluación y decisión de eventos en seguridad de la información	x			**3**
Respuesta a incidentes en seguridad de la información	x			**3**
Aprendizaje de los incidentes en seguridad de la información	x			**2**
Recolección de evidencia	x			**2**

Se identifican procesos con responsables a cargo de identificar, evaluar y definir las acciones ante los incidentes en torno a la seguridad de la información asegurando una adecuada gestión de los mismos.

Sin embargo, existen algunas oportunidades de mejora en cuanto al aprendizaje y recolección de evidencia al momento de presentarse algún incidente. A pesar que el departamento de TI toma acciones al momento de percibir un alto impacto en un incidente y se registran evidencias, las mismas no se tienen de forma centralizada ni se cuenta con documentación en ninguno de los dos controles.

Generar acciones para atender las oportunidades de mejora alineadas a lo establecido por la International Organization for Standardization (2013b) permite a la organización asegurar una adecuada gestión de los incidentes y eventos relacionados con la seguridad de la información desde una perspectiva coherente y eficaz.

4.1.2.13. Seguridad de la Información en la Gestión de Continuidad del Negocio.

La **Tabla 22** muestra los controles relacionados con la seguridad de la información en la gestión de la continuidad del negocio donde se observa un cumplimiento en los aspectos de planificación, implementación y verificación de dicha continuidad.

Tabla 22. *Seguridad de la Información en la Gestión de Continuidad del Negocio.*

Controles	Sí	No	N/A	Estado actual
Planificación de la continuidad de la seguridad de la información	X			**3**
Implementar la continuidad de la seguridad de la información	X			**3**
Verificar, revisar y evaluar la continuidad de la seguridad de la información	X			**3**
Disponibilidad de los recursos de tratamiento de la información		x		**1**

Por otra parte, se identifica la falta de acciones de control que permitan garantizar la disponibilidad de los recursos de tratamiento de la información, provocando limitantes en la operación ante situaciones adversas y riesgos relacionados con la integridad o confidencialidad de la información.

Según la International Organization for Standardization (2013b), atender las necesidades identificadas permite a la organización gestionar adecuadamente la seguridad de la información, garantizando así la integridad, confidencialidad y disponibilidad de los recursos que sean necesarios en situaciones adversas donde se requiera de una continuidad efectiva del negocio.

4.1.2.14. Cumplimiento. Como se muestra en la **Tabla 23**, la organización mantiene los controles de cumplimiento debidamente implementados en los que se tienen procesos definidos, documentados y con sus respectivas revisiones.

Tabla 23 *Cumplimiento.*

Controles	Sí	No	N/A	Estado actual
Identificación de la legislación aplicable y los requisitos contractuales	X			**3**
Derechos de propiedad intelectual	X			**3**
Protección de los registros de la organización	X			**3**
Privacidad y protección de la información de carácter personal	X			**3**
Regulación de controles criptográficos	X			**3**
Revisión independiente de la seguridad de la información	X			**3**
Cumplimiento con políticas y estándares de seguridad	X			**3**
Revisión de cumplimiento técnico	X			**3**

Según el objetivo que menciona la International Organization for Standardization, (2013b), mantener los respectivos controles previene a la organización sobre un posible incumplimiento de obligaciones legales, reglamentarias o contractuales con respecto a los requerimientos correspondientes a la seguridad de la información.

4.1.2.15. Gestión de Riesgos. Con respecto a la gestión de riesgos se observa un cumplimiento parcial en la identificación de riesgos y se verifica la ausencia de acciones en la mayoría de los controles como se muestra en la **Tabla 24**.

Tabla 24. *Gestión de Riesgos.*

Controles	Sí	No	N/A	Estado actual
¿Existe un proceso de gestión de riesgos documentado, alineado a la organización, con criterios definidos y debidamente aprobado por la dirección?		x		**1**
¿Se define un alcance que incluya objetivos, resultados esperados, tiempos, recursos y herramientas de evaluación para el proceso de gestión de riesgos?		x		**1**
¿Se definen los riesgos con sus criterios de aceptación de acuerdo a los objetivos de la organización y se identifican las causas y consecuencias asociadas a cada uno de los riesgos?		x		**1**
¿Se identifican los riesgos para la seguridad de la información para la organización y las instalaciones de procesamiento de información relacionados a procesos comerciales, partes externas o clientes y se implementan los controles adecuados antes de otorgar acceso?	X			**2**
¿Se encuentran controles para cada riesgo debidamente clasificados en: predicción, prevención, detección y corrección?		x		**2**
¿Se cuenta con escenarios establecidos en los que se identifiquen los diferentes eventos, las amenazas y los activos que se pueden ver afectados?		x		**1**

Controles	Sí	No	N/A	Estado actual
¿La organización cuenta con un seguro de responsabilidad comercial general?		x		1
¿La organización tiene actualmente cobertura de seguro de responsabilidad profesional?		x		1
¿Se cuenta con un responsable del proceso a cargo del plan de acción, plan de respuesta y actualización de la gestión?	X			1
¿Se realizan las revisiones al proceso periódicamente?		x		1

El Departamento de TI realiza una identificación de los riesgos, sin embargo se realiza de manera informal, realizando evaluaciones de las vulnerabilidades que permiten la toma de decisiones en la implementación de controles para el acceso a la información y determinando los riesgos asociados a los diferentes involucrados como resultado de dicha evaluación.

En cuanto a la clasificación de los riesgos se cuenta con la detección ante accesos desde direcciones IP desconocidas, sin embargo no se realizan clasificaciones de manera adecuada para cumplir con los requerimientos que solicitan los clientes.

Es importante que la organización tome acciones de manera inmediata para atender las falencias presentadas que permita cumplir tanto con los requerimientos de los clientes como de los respaldos necesarios en los controles especificados por la norma ISO 27001:2013.

Actualmente el departamento cuenta con un responsable a cargo de desarrollar un proceso para la gestión de riesgos. El mismo estará basado en la norma ISO 27005:2018 y se

pronostica que se tendrá definido, documentado, aprobado y comunicado para finales del presente año.

Esto demuestra el compromiso adquirido por la organización para atacar las brechas encontradas bajo estándares que se alineen con el sistema de gestión de la seguridad de la información.

4.1.2.16. Privacidad. El área de privacidad muestra, en la **Tabla 25**, los controles definidos para la verificación de cumplimiento, los cuales fueron obtenidos del Apéndice F. Identificación de Requerimientos de Clientes..

Tabla 25. *Privacidad.*

Controles	Sí	No	N/A	Estado actual
¿El sistema implica la recopilación de datos personales de los usuarios?	X			**3**
¿La información personal es revelada o retenida por terceros?			x	**N/A**
¿Se cuenta con una política de privacidad establecida?	X			**3**
¿Existen salvaguardias para garantizar el cumplimiento de las leyes nacionales o regionales pertinentes con respecto a la transferencia transfronteriza de información?	X			**3**

Al realizar la verificación se encuentra un control, el cual no aplica para la organización al no realizar ninguna manipulación o retención de información de terceros en ninguno de sus procesos o servicios. Para el resto de los controles se documentan cumplimientos adecuados, los cuales incluyen el correcto tratamiento de la información de terceros, la documentación

adecuada de políticas de privacidad y el cumplimiento de la legislación establecida por cada país en materia de transferencia de información.

Contar con acciones adecuadas en esta área brinda a la organización y los clientes una mayor confianza en la seguridad con que es tratada la información sensible y datos personales en los procesos del negocio.

4.1.2.17. Tercerización. En el área de tercerización tomada del Apéndice F. Identificación de Requerimientos de Clientes. y mostrada en la siguiente **Tabla 26**, se identifica el siguiente estado actual de sus controles.

Tabla 26. *Tercerización.*

Controles	Sí	No	N/A	Estado actual
¿Existe una política para la gestión de riesgo relacionados a terceras partes?		x		**1**
¿Se encuentran los contratos relacionados a terceras partes debidamente documentados?	X			**3**
¿Existe un acuerdo de confidencialidad con todos los proveedores?	X			**3**

Como se observa la organización cuenta con implementación de controles al momento de generar y documentar los contratos con terceras partes en los que se incluya los respectivos acuerdos de confidencialidad que garanticen la seguridad de la información en los procesos y servicios adquiridos.

A pesar que actualmente no se cuenta con acciones en la identificación de los riesgos relacionados con terceras partes, la organización tiene presente esta mejora como una

prioridad para ser tomada en cuenta en el proceso de gestión de riesgos que se encuentra en desarrollo.

Mantener un alcance total de los controles en esta área permite a la organización garantizar una adecuada gestión en el cumplimiento de las cláusulas contractuales y la seguridad de la información al momento de adquirir los servicios de otras empresas.

4.1.2.18. Servicios en la Nube. Según lo establecido en el Apéndice F. Identificación de Requerimientos de Clientes. y como última área de verificación tomada en cuenta para la elaboración del sistema de gestión de la seguridad de la información se evalúan los controles relacionados con servicios en la nube mostrados en la **Tabla 27**.

Tabla 27. *Servicios en la Nube.*

Controles	Sí	No	N/A	Estado actual
¿Existe una política para la computación en la nube definida por la organización?		x		**1**
¿Su instancia está configurada como una subred privada para segregar sus datos de otros clientes?	x			**3**
¿La organización gestiona la clave de cifrado en la nube?	x			**3**

Como se puede observar la organización cuenta con controles en la red, tomados en cuenta también en la sección 4.1.2.9. Seguridad de las Comunicaciones de este capítulo en los controles que especifica ISO 27001:2013 para la segregación de redes, implementando la seguridad necesaria a través de subredes y máquinas virtuales definidas para cada cliente en específico. Además se realiza una adecuada gestión de la clave de cifrado a través de la herramienta de Microsoft Azure de acuerdo con los recursos creados o requeridos por cada

cliente, brindando la seguridad de la información y los recursos de tratamiento de la misma, necesarios para cada proyecto.

A pesar que la organización presenta brechas en el establecimiento de una política debidamente documentada, actualmente se encuentra un proyecto en desarrollo enfocado precisamente en atender las necesidades presentadas en el control de los procesos de servicios en la nube.

4.1.3. Análisis de Brechas y Capacidad

Una vez se realizó la verificación de todos los controles y se definió su estado actual se procede a realizar un análisis de las brechas encontradas.

Para calcular estas brechas se toma la valoración asignada en el estado actual de los controles, realizando un cálculo de la puntuación total que tendrá cada área de acuerdo con la cantidad de controles que tenga y posteriormente realizando una ponderación de acuerdo con las valoraciones obtenidas en el estado actual de cada control para obtener un porcentaje que corresponde al nivel de cumplimiento por área.

A continuación se muestran las fórmulas empleadas para el cálculo de las brechas, las cuales surgen como resultado del grupo focal evidenciado en el Apéndice C. Grupos Focales. – Apartado: Tabla C1.

Primero se define la calificación total para cada área, tomando en cuenta la cantidad de controles y multiplicándose por la puntuación máxima que puede alcanzar cada control en su estado actual, como se muestra a continuación.

$$Cantidad\ de\ controles\ del\ área * 3 = Calificación\ total\ del\ área$$

Una vez se establecen las calificaciones totales que corresponden a cada área de control se procede con la siguiente fórmula que permita determinar el porcentaje de cumplimiento en cada área.

$$\frac{Calificación\ obtenida\ por\ área * 100}{Calificación\ total\ del\ área} = Porcentaje\ de\ cumplimiento\ por\ área$$

Al ser aplicadas las fórmulas anteriores a cada una de las áreas evaluadas se obtuvieron los resultados que se muestran en la **Tabla 28.** Análisis de Brechas y Capacidad, los cuales se integran con los niveles de capacidad COBIT 2019 especificados en la sección ***3.6.7. Análisis de Capacidad*** del capítulo III en este documento, con el objetivo de realizar una priorización de las brechas que se encuentre respaldado por criterios de evaluación semicuantitativos.

Tabla 28. *Análisis de Brechas y Capacidad*

Número de área	Área de control	Calificación total del área. (100%)	Puntuación de controles obtenida por área.	Porcentaje de cumplimiento por área.	Nivel de capacidad
1	Políticas en seguridad de la información	6	6	100%	Completamente
2	Organización de la seguridad de la información	21	14	66%	Largamente
3	Seguridad de los recursos humanos	18	16	88%	Completamente
4	Administración de activos	30	18	60%	Largamente
5	Control de accesos	42	39	92%	Completamente
6	Criptografía	6	4	66%	Largamente
7	Seguridad física y ambiental	45	44	97%	Completamente
8	Seguridad de las operaciones	42	39	92%	Completamente
9	Seguridad de las comunicaciones	21	19	90%	Completamente

Número de área	Área de control	Calificación total del área. (100%)	Puntuación de controles obtenida por área.	Porcentaje de cumplimiento por área.	Nivel de capacidad
10	Adquisición, desarrollo y mantenimiento de sistemas	39	39	100%	Completamente
11	Relación con proveedores	15	9	60%	Largamente
12	Gestión de incidentes de seguridad de la información	21	19	90%	Completamente
13	Seguridad de la información en la gestión de la continuidad del negocio	12	10	83%	Largamente
14	Cumplimiento	24	24	100%	Completamente
15	Gestión de riesgos	30	12	40%	Parcialmente
16	Privacidad	9	9	100%	Completamente
17	Tercerización	9	7	77%	Largamente
18	Servicios en la nube	9	7	77%	Largamente

Al realizar un análisis de los resultados obtenidos se determina que para alcanzar un nivel de capacidad de “Largamente” como primer paso, se requieren concentrar los esfuerzos en atender el área correspondiente a la gestión de riesgos.

Tomando en cuenta los niveles de capacidad y los porcentajes de cumplimiento obtenido por cada área se realiza la siguiente priorización de brechas, las cuales contemplan tanto los requerimientos enviados por los clientes de la empresa como los establecidos por la norma ISO 27001:2013 para optar por la certificación.

4.1.4. Priorización de Brechas.

La priorización de las brechas que se muestra en la **Tabla 29** se encuentra establecida bajo los resultados que fueron mostrados en la anterior **Tabla 28**, de forma que se priorizan las

áreas que requieren de acciones para solventar las necesidades encontradas según su porcentaje actual de cumplimiento obtenido.

Tabla 29. *Priorización de Brechas.*

Área de control	Porcentaje de cumplimiento por área.
Gestión de riesgos	40%
Relación con proveedores	60%
Administración de activos	63%
Organización de la seguridad de la información	67%
Criptografía	67%
Tercerización	78%
Servicios en la nube	78%
Seguridad de la información en la gestión de la continuidad del negocio	83%
Seguridad de los recursos humanos	89%
Seguridad de las comunicaciones	90%
Gestión de incidentes de seguridad de la información	90%
Control de accesos	93%
Seguridad de las operaciones	93%
Seguridad física y ambiental	98%
Políticas en seguridad de la información	100%
Adquisición, desarrollo y mantenimiento de sistemas	100%
Cumplimiento	100%
Privacidad	100%

Tomando en cuenta los resultados observados anteriormente, se establece que el Departamento de TI debe concentrar sus esfuerzos en el área de gestión de riesgos, la cual presenta una carencia de un procedimiento definido e implementado que responda a las políticas y controles del SGSI.

Como parte del compromiso de mejora que el departamento muestra en su objetivo de optar por la certificación en la norma ISO 27001:2013, actualmente se cuenta con un responsable a cargo de desarrollar el debido proceso para la gestión de riesgos, el cual se pretende definir según lo establecido por la norma ISO 27005:2018 de forma que se mantenga la estandarización adecuada de los procesos bajo la serie de normas ISO/IEC 27000.

Avanzar en las siguientes áreas según el orden de prioridad establecido será el siguiente paso para lograr que se pueda alcanzar un nivel de capacidad de “Completamente” para todas las áreas, de forma que se pueda garantizar una gestión de la seguridad de la información de manera holística.

De esta manera se plantearán las respectivas propuestas que atiendan las brechas identificadas en las áreas que tienen un nivel de cumplimiento menor al 85%, de forma que sea posible llevar todas las áreas de control a un nivel de capacidad “Completamente” como primer paso hacia la preparación para las respectivas auditorías que permitan otorgar la certificación ISO 27001:2013.

Una vez se cierren las brechas identificadas el Departamento de TI estará preparado para contratar los servicios de consultoría y auditoría brindados por las organizaciones encargadas de emitir la certificación ISO 27001:2013.

4.2. Conclusiones del Análisis de Situación Actual.

Al realizar las respectivas reuniones iniciales con la organización, se determina la necesidad que presenta el departamento TI en lograr una futura certificación bajo la norma ISO 27001:2013 que acredite su correcta gestión de la seguridad de la información.

- Se requiere alinear el sistema de gestión de seguridad de la información (SGSI) a lo establecido por la norma ISO 27001:2013 para optar por la certificación que desea la organización.
- El SGSI debe contemplar los requerimientos de los clientes de forma que satisfaga las necesidades y preocupaciones en torno a la seguridad de la información.
- Se determina que el SGSI debe evaluar todos los controles especificados en el Anexo A de la norma ISO 27001:2013 para determinar los controles que apliquen a los diferentes procesos de negocio en la organización.
- Se logra observar un cumplimiento total en las áreas de:
    - Políticas en seguridad de la información.
    - Adquisición, desarrollo y mantenimiento de sistemas.
    - Cumplimiento
    - Privacidad
- Para las cuales se establece que no requieren de acciones inmediatas y se deben mantener bajo la monitorización correspondiente que permita la mejora continua de los procesos y controles.
- A partir de la priorización de brechas se logra determinar que el área que requiere principal atención es gestión de riesgos, al no contar con un proceso establecido donde se identifiquen y documenten los riesgos y las acciones que la organización debe establecer para cada riesgo asociado a la seguridad de la

información, de forma que se atiendan tanto lo estipulado por la norma ISO 27001:2013 como los requerimientos demandados por los clientes.

- Actualmente el departamento cuenta con un responsable a cargo de definir el proceso correspondiente a la gestión de riesgos, lo que demuestra el compromiso adquirido para alcanzar los requerimientos necesarios para la certificación.
- Una vez se atienda esta necesidad crítica se deben atacar las brechas encontradas en las áreas con un nivel de cumplimiento menor al 85%, tomando como referencia la priorización establecida.
- Los resultados obtenidos son producto del estudio de las normas ISO 27001:2013 e ISO 27002:2013, las políticas internas de la organización, el cuestionario con requerimientos de clientes y las diferentes reuniones para la debida verificación; los cuales permitieron establecer los hallazgos presentados y definir las recomendaciones que permitan atender los riesgos encontrados y aplicar las acciones correspondientes para atender las diferentes necesidades.

Capítulo V: Propuesta de Solución

En el siguiente capítulo se detallan las secciones que componen el caso de negocio correspondiente a la propuesta de solución presentada para el Departamento de TI.

5.1. Resumen ejecutivo

En la siguiente **Tabla 30** se presenta un resumen ejecutivo correspondiente al caso de negocio desarrollado.

Tabla 30 *Resumen Ejecutivo*

Fecha
20 de septiembre de 2021
Nombre del proyecto
Propuesta de viabilidad mediante un caso de negocio para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013.
Problemas identificados
• Falta de estandarización en el proceso de gestión de seguridad de la información. • Falta de eficiencia y calidad en el proceso de validación de controles. • Requerimientos más estrictos por parte de los clientes.
Descripción del caso de negocio
En el siguiente caso de negocio se definen las actividades necesarias de implementar que atiendan las brechas identificadas en seguridad de la información de manera que se pueda preparar al Departamento de TI con miras a la auditoría de certificación ISO 27001:2013.
Objetivo general del caso de negocio
Ofrecer una propuesta para la implementación de un sistema de gestión de seguridad de la información en el Departamento de TI con miras a certificación en la norma ISO 27001:2013.
Objetivos específicos del caso de negocio
• Estandarizar el proceso de gestión de seguridad de la información. • Definir los aspectos clave para contar con la calidad y eficiencia en el proceso de gestión de seguridad de la información. • Definir las acciones necesarias para establecer los controles que brinden la seguridad requerida por el SGSI.
Equipo de desarrollo

El proyecto será desarrollado por el Departamento de TI a cargo de los siguientes responsables.

- Director de Seguridad.
- Analista de Negocio de TI.
- Ingeniero de Procesos.
- Auditor Interno.

5.1.2. Importancia y Propósito

El siguiente caso de negocio presenta los diferentes análisis y estudios necesarios que permitan determinar los aspectos que el Departamento de TI debe tomar en cuenta para la correcta implementación de un sistema de gestión de seguridad de la información el cual atienda las brechas identificadas de forma que se ejecuten las actividades con los respectivos recursos que permitan preparar a la organización para optar a la certificación en la norma ISO 27001:2013.

Para la organización es importante cumplir con estándares en gestión de la seguridad de la información que le permitan garantizar a sus clientes que los datos sensibles serán tratados de manera adecuada.

Mantener un proceso de gestión de seguridad de la información debidamente implementado y estandarizado permite al Departamento de TI cumplir con los indicadores clave de rendimiento especificados en la **Tabla 2**, en relación con la calidad y eficiencia de sus procesos.

Una mayor eficiencia en las operaciones permite ofrecer a los clientes de la organización mejores tiempos de entrega al tener una mayor productividad y disminución en los incidentes a partir de la adecuada gestión de riesgos relacionados con la seguridad de la información.

A través de un responsable que esté encargado de llevar a cabo las diferentes fases (PHVA) que garanticen la mejora continua del SGSI, el Departamento de TI podrá mantener su

proceso debidamente implementado y actualizado a lo largo de todo su ciclo de vida al definir los controles y políticas que respondan a los requerimientos o necesidades que surjan en la organización.

5.3. Propuesta de solución

Para determinar la viabilidad de la propuesta planteada en este caso se realizan los siguientes estudios y análisis que permitan abordar las necesidades presentadas por la organización así como los diferentes aspectos que deben ser tomados en cuenta para su implementación.

5.3.1. Estudio de Mercado

El presente proyecto requiere de una investigación de mercado que permita conocer la necesidad de la propuesta planteada para la organización, lo cual se pretende conseguir con el desarrollo del siguiente estudio de mercado.

5.3.1.1. Objetivos De Estudio De Mercado. A continuación se especifican los objetivos de este estudio.

- Determinar la necesidad del departamento de TI para obtener una certificación en seguridad de la información.
- Identificar las opciones que ofrece el mercado en cuanto a la certificación de organizaciones en seguridad de la información.
- Definir la estrategia de distribución para el SGSI hacia las partes involucradas.

5.3.1.2. Definición Del Sistema de Gestión de Seguridad de la Información. En esta sección del estudio se caracteriza el sistema de gestión de seguridad de la información alineado a la norma ISO 27001:2013 requerido para optar a la futura certificación que se desea obtener.

La norma ISO 27001:2013 establece catorce áreas que especifican 144 controles que pueden implementar las organizaciones para su adecuada gestión de la seguridad de la información.

Además, como parte de la alineación del sistema con los requerimientos de los clientes, se toma como referencia el Apéndice F. Identificación de Requerimientos de Clientes. que contiene la recopilación de los requerimientos enviados por los clientes a través de cuestionarios para la verificación por parte de la organización.

Al analizar dichos requerimientos se identifica una similitud con lo establecido en la norma ISO 27001:2013 en su mayoría, sin embargo se destacan cuatro áreas con veinte controles que deben ser tomadas en cuenta para agregar los controles en el SGSI que respondan a esas áreas y requerimientos específicos de forma que se logre una verificación holística, tomando en cuenta lo establecido por la industria, las necesidades del departamento de TI y los requerimientos de los clientes.

Las áreas del SGSI que son evaluadas se mencionan a continuación.

1. Políticas de seguridad de la información.
2. Organización de seguridad de la información
3. Seguridad ligada a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del ambiente.

8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de los sistemas de información.
11. Relaciones con los proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
14. Cumplimiento.
15. Gestión de riesgos.
16. Privacidad.
17. Tercerización.
18. Servicios en la nube.

El SGSI definido a través de las áreas mencionadas contiene un total de 164 controles que serán verificados en reuniones con los colaboradores del Departamento de TI y tomando como referencia la guía de implementación presentada en la norma ISO 27002:2013, así como el Apéndice F. Identificación de Requerimientos de Clientes. correspondiente a los requerimientos enviados por los clientes, de forma que sea posible determinar el nivel de cumplimiento en cada uno de los controles a partir de las observaciones y comentarios de los colaboradores. Con esto se pretende tener un panorama claro de las acciones que se deben tomar por la organización para mitigar los riesgos y vulnerabilidades que se presentan en materia de seguridad de la información.

En dicha verificación se realiza una identificación de los controles cumplidos, los controles no cumplidos y aquellos que no apliquen por la naturaleza y operaciones del negocio. En cada verificación se documentan los comentarios obtenidos por parte de los colaboradores que corresponden a las acciones que se toman para cumplir con los controles especificados por el SGSI.

El sistema contiene una evaluación del estado actual de cada control que permita realizar la ponderación de las áreas y establecer las brechas encontradas.

Además, mapea los apartados, cláusulas o estatutos encontrados en la documentación de las políticas internas con las que cuenta la organización que corresponden con acciones para cumplir con los diferentes controles.

El sistema permite al departamento tener una visión holística de la situación en la que se encuentra la seguridad de la información, tomando en cuenta lo establecido por las normas ISO 27001:2013 e ISO 27002:2013, así como los principales requerimientos de los clientes al momento de contratar los servicios de la empresa, agilizando el proceso de gestión de la seguridad de la información y el proceso de verificación de controles.

Característica	Descripción
Áreas y controles ISO 27001:2013	La norma ISO 27001:2013 establece catorce áreas que especifican 144 controles los cuales fueron incluidos en el SGSI.
Requerimientos de clientes	A partir del análisis de los requerimientos enviados por los clientes se agregan cuatro áreas más que cuentan con veinte controles, todos incluidos en el SGSI.
Verificación de cumplimiento	El sistema permite la identificación de los controles que cumplen, no cumplen y aquellos que no aplican.
Mapeo de documentación	Se identifican las cláusulas o políticas con su respectivo apartado para los controles

Característica	Descripción
	que cuentan con su debida documentación.
Controles existentes y observaciones	Se documentan los controles existentes según lo especificado por la guía de cumplimiento de la norma ISO 27002:2013 y las respectivas observaciones obtenidas en la auditoría de cumplimiento.
Estado Actual	Se evalúa el estado actual de cada control con una calificación mínima de uno en caso de no cumplir con el control, dos en caso de presentar oportunidades de mejora y tres para los controles debidamente implementados.
Brechas	De acuerdo con los controles faltantes y las observaciones recibidas se establecen las brechas que deben ser atendidas según el área de control.
Nivel de capacidad	Se establecen los niveles de capacidad definidos por COBIT 2019 de acuerdo al nivel de cumplimiento obtenido por área.

5.3.1.3. Análisis De La Demanda. Para realizar un análisis de la demanda se consultan tanto fuentes primarias como secundarias las cuales respaldan la necesidad de un sistema de gestión de seguridad de la información, el cual permita al Departamento de TI cumplir con los requerimientos para la certificación en la norma ISO 27001:2013.

5.3.1.3.1. Fuentes y Sujetos de información por consultar. A continuación se mencionan los sujetos de información, fuentes primarias y secundarias por consultar.

- Fuentes primarias: norma ISO 27001:2013, norma ISO 27002:2013, Director de Seguridad, Analista de Negocio, Analista de Negocio CRM, Administrador de Proyectos.
- Fuentes secundarias: Reporte INTERPOL 2020, reporte de seguridad ESET 2021

5.3.1.3.2. Fuentes primarias. Como principal fuente primaria se toma como referencia lo establecido por la norma ISO 27001:2013 la cual permite identificar el contexto en materia de seguridad de la información, de forma que se puedan establecer los controles y procedimientos alineados a la organización. Además de la norma ISO 27002:2013 que establece una guía para la adecuada implementación y monitorización de los controles, políticas y procedimientos definidos para el SGSI.

A través de las consultas realizadas a los diferentes colaboradores del Departamento de TI se identifica una necesidad interna de la organización por definir un sistema de gestión de la seguridad de la información que atienda las solicitudes de los diferentes grupos de involucrados con sus respectivos intereses, problemas percibidos y mandatos o recursos que aporten para determinar la demanda como se muestra en la **Tabla 31** con las percepciones de grupos de involucrados sobre un SGSI a continuación.

Tabla 31 *Percepciones de grupos de involucrados*

Grupo de Involucrados	Intereses	Problemas percibidos	Mandatos y recursos
Alta Gerencia	Proteger productos y propiedad intelectual	Ninguno	Destinar presupuesto.
Departamento de Éxito de clientes	Garantizar la satisfacción de los clientes.	Ninguno	Objetivo estratégico del departamento. Indicadores clave de rendimiento.
Colaboradores del departamento de TI	Mantener controles y métricas eficientes en seguridad de la información. Estandarización del proceso de seguridad de la información.	Requerimientos más estrictos por parte de los clientes. Descentralización de los esfuerzos en seguridad.	Brindar conocimiento de los procesos. Controles y políticas.
Departamento de producto	Reducir las vulnerabilidades en los procesos de migración.	Vulnerabilidades de red en ambientes de producción.	Ninguno

Clientes	Obtener un producto eficiente y de calidad. Mantener sus datos y código fuente protegidos.	Ninguno	Requerimientos
Colaboradores de otros departamentos	Conocimiento para no comprometer la seguridad de la información.	Se identificó acceso a cuentas de correo y envío de *phishing*.	Ninguno

Fuente: Apéndice N. Minutas de Reuniones con la Organización. – Tabla N17. Identificación de las percepciones de grupos de involucrados

5.3.1.3.3. Factores críticos. A partir del grupo focal realizado en reunión con el Analista de Negocio de TI y Analista de Negocio CRM (ver Apéndice C. Grupos Focales. – Apartado: Tabla C2) se identifican los siguientes factores críticos para obtener la certificación.

- **Disponibilidad e interés del responsable o equipo ejecutor:** se deben asignar los responsables o equipo de trabajo dedicado a realizar las diferentes actividades. Contar con la disponibilidad de personal en el departamento de TI que pueda dedicar el tiempo suficiente para el desarrollo de las tareas será un elemento clave para lograr los objetivos en el plazo establecido.

- **Mercado:** mejorar el posicionamiento en el mercado a través de un proceso de gestión de la seguridad de la información que se encuentre certificado es un aspecto de gran importancia para generar una mayor confianza y satisfacción de los clientes.

- **Eficiencia:** agilizar los procesos y operaciones en la organización, además de mantener los ambientes con la seguridad adecuada permite una mayor productividad al mismo tiempo que disminuye los costos operativos.

- **Anticipación:** la diversidad de industrias a las que pertenecen los clientes de la empresa y el creciente número de ataques informáticos preocupan a la organización y aumentan la rigurosidad en los requerimientos recibidos. Tomar acciones para garantizar la seguridad de la información previene a la empresa de posibles incidentes.

- **Formación y capacitación:** mantener a los usuarios del SGSI debidamente capacitados para garantizar la correcta implementación y monitorización del sistema.

- **Concientización:** realizar los programas de concientización permite que los colaboradores de la organización comprendan la importancia que tiene preservar la seguridad de la información en todos los procesos de negocio, de forma que las políticas y controles sean adoptados de una manera proactiva.

Al tratarse de un proyecto que requiere de inversiones en tiempo y mano de obra para el desarrollo de procesos y políticas necesarias para el sistema de gestión de seguridad de la información y sabiendo que el proceso de certificación también requiere de constantes inversiones para garantizar la mejora continua y realizar las respectivas acreditaciones, se consideran estos factores críticos para asegurar el éxito del proyecto.

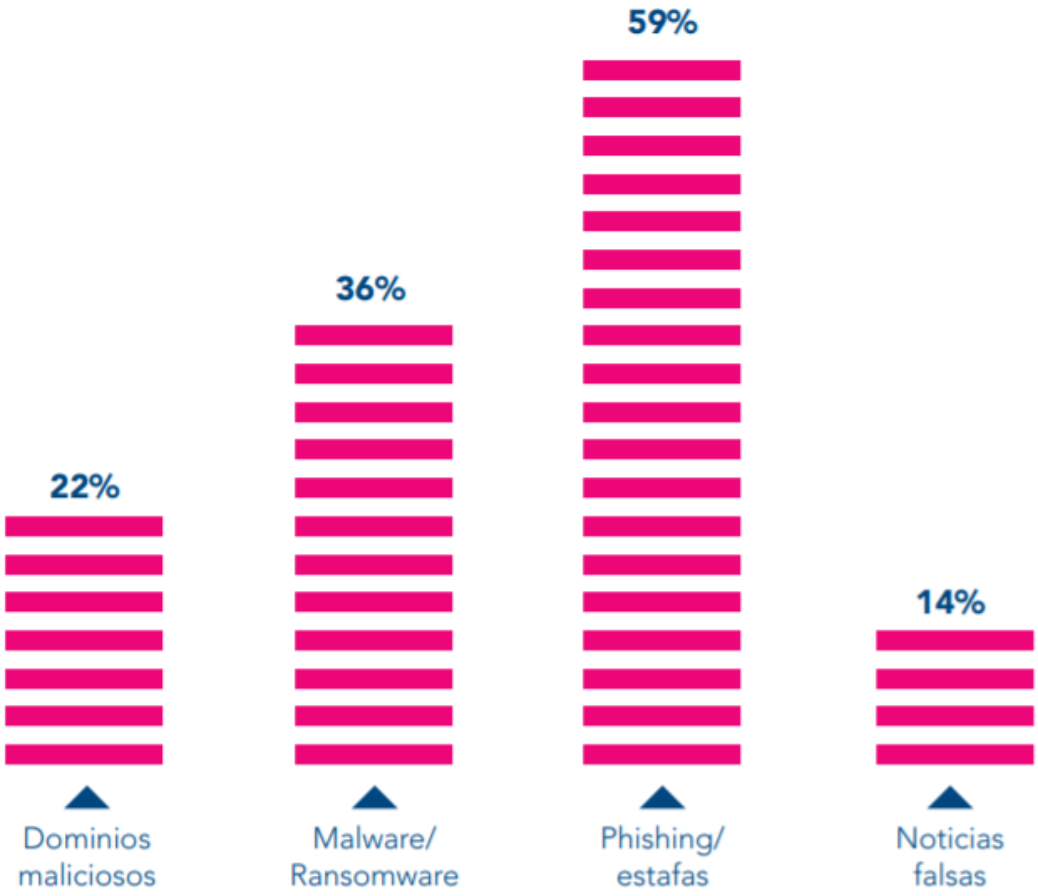
5.3.1.3.4. Fuentes secundarias. Actualmente la situación global que se vive a raíz de la pandemia por la COVID-19 ha provocado un aumento en los ciberataques que mantiene preocupadas a las organizaciones internacionales.

En un informe realizado por la Organización Internacional de Policía Criminal (INTERPOL), muestra un aumento en las amenazas percibidas, esto debido a la necesidad de las empresas en implementar el teletrabajo como contingencia ante la pandemia, lo que provoca un aumento de los riesgos debido a posibles vulnerabilidades en la red que los hackers pueden aprovechar para tener acceso remoto a la información y poner en peligro la seguridad (INTERPOL, 2020).

Los correos electrónicos con aparente información acerca de la COVID-19 han aumentado los casos de *phishing* y estafas, así como también los dominios maliciosos que utilizan estas palabras clave para aprovechar la gran cantidad de personas que buscan información sobre la COVID-19 (INTERPOL, 2020).

Este informe también resalta que empresas medianas, como es el caso de Mobilize.Net, están siendo víctimas de ataques por medio del *ransomware Lockbit*, el cual provoca un bloqueo en el acceso a los sistemas por parte de los hackers, quienes solicitan un pago para la devolución del acceso, provocando un riesgo de suma importancia en el aseguramiento de la confidencialidad (INTERPOL, 2020).

A continuación se muestra un gráfico que muestra los resultados de análisis de datos de los diferentes países miembros de la INTERPOL, los socios privados, y el Centro de Intercambio de Información sobre la Ciberdelincuencia; el cual muestra las principales ciberamenazas identificadas actualmente.



Fuente: Tomado de INTERPOL, 2020.

Como también lo menciona el reporte publicado por ESET (2021), la nueva normalidad que impuso la pandemia provoca que las organizaciones modifiquen sus prioridades y establezcan las condiciones necesarias que atiendan adecuadamente la seguridad de la información.

El estudio también muestra que existe un aumento de las preocupaciones por parte de las empresas en cuanto a los riesgos de seguridad que puedan generar los factores humanos debido a que el nivel de riesgo que genera el teletrabajo es equivalente al provocado por los ciberataques (ESET, 2021).

Dentro de los hallazgos más importantes que muestra el reporte destacan:

- La principal preocupación y la primera causa de incidentes de seguridad en las empresas latinoamericanas son los códigos maliciosos.
- Los ataques dirigidos a través de *ransomware* se volvieron más agresivos.
- La cantidad de ataques a los servicios de acceso remoto por medio de la fuerza bruta creció un 704%.
- La utilización de dispositivos móviles para actividades corporativas genera vulnerabilidades al no presentar soluciones antimalware en dichos dispositivos (ESET, 2021).

Tomando en cuenta las preocupaciones expresadas en los reportes anteriores se puede determinar que existe una demanda insatisfecha que requiere atender la seguridad de la información a partir de un sistema que permita su adecuada gestión.

5.3.1.4. Análisis de la oferta. Con el propósito de realizar el correcto análisis de la oferta se identifica para el presente proyecto una oferta de tipo competitiva o de mercado libre que como menciona Baca, (2016) corresponde con aquellos productores de artículos o servicios que se encuentran en circunstancias de libre mercado donde existen múltiples productores que determinan su participación en el mercado de acuerdo con la calidad, precio y servicio que ofrecen al consumidor.

Para el presente caso se evalúan las organizaciones que brindan la acreditación en la norma ISO 27001:2013 las cuales ofrecen los respectivos servicios de consultoría y soporte para la preparación de la empresa que desea obtener la certificación, de forma que se pueda comparar los servicios brindados en términos de su localización, calidad y precio de los productos.

En la siguiente **Tabla 32** se muestran los aspectos considerados para los tres proveedores evaluados.

Tabla 32. *Análisis de proveedores de certificación*

Proveedor	Localización	Calidad	Precio
INTECO	Costa Rica	- Membresía de normas ISO - Membresía IQ-NET - Membresía Copant	$25.000
BSI Group	Reino Unido	- *American National Standards Institute - American Society for Quality National Accreditation Board LLC (ANAB)*	Cotización pendiente
EQA	México	- *American National Standards Institute - American Society for Quality National Accreditation Board LLC (ANAB)*	Cotización pendiente

Al realizar el análisis de los proveedores mostrados anteriormente es importante tomar en cuenta que la única opción que cuenta con oficinas físicas en el país es el Instituto de Normas Técnicas de Costa Rica INTECO, aspecto que puede ser relevante coordinar y recibir las debidas auditorías presenciales en la empresa.

En cuanto a la calidad del servicio el instituto cuenta con acreditación de IQNet que garantice la credibilidad y confianza en el proceso de capacitación y certificación de productos, procesos, personas y servicios.

A pesar que los demás proveedores cuentan con acreditaciones internacionales que aseguren la calidad de sus servicios se pueden presentar algunas limitaciones que deban ser consideradas al momento de realizar las respectivas auditorías que podrían afectar el precio final del servicio. Sin embargo ambos ofrecen servicios de auditoría tanto virtual como presencial.

Con respecto al precio, a pesar que fueran enviados los respectivos formularios de solicitud de cotización, como se muestran en el Apéndice I. Cotización EQA.y Apéndice J. Cotización BSI Group., al momento de finalizar este documento, solo fue posible obtener la cotización por parte de INTECO (ver Apéndice K. Cotización INTECO.).

5.3.1.5. Estrategia de comercialización. Al hablar de la comercialización de un producto no se debe entender simplemente como el proceso por el cual se distribuye el producto hacia el consumidor o usuario final, sino establecer los aspectos del lugar y momento adecuados de forma que se logre la satisfacción esperada en el cliente (Baca Urbina, 2016).

Al establecer el sistema de gestión de seguridad de la información como producto final y activo de la organización se debe brindar una estrategia de comercialización que cumpla con los aspectos mencionados anteriormente, donde se definan las acciones y herramientas que permitan hacer llegar el SGSI a los diferentes usuarios de la manera adecuada.

La organización cuenta con sistemas que le permiten comunicar de manera efectiva y formal a los colaboradores de la organización la disponibilidad del SGSI como se muestra a continuación.

- **Microsoft SharePoint:** La organización mantiene la mayoría de sus operaciones empresariales a través de la plataforma de Microsoft SharePoint en la que tiene todos sus documentos, políticas e información interna de conocimiento para todos sus colaboradores de forma centralizada, la cual sería el lugar adecuado en donde se almacenará y se tendrá a disposición de los respectivos usuarios el SGSI.
- **Correo electrónico:** A través del correo electrónico de la organización se realizará la respectiva comunicación a los diferentes usuarios, departamentos y partes interesadas de la publicación oficial del SGSI en el SharePoint.

- **Publicidad:** Generar la promoción adecuada de la certificación a través de la página web y las diferentes redes sociales de la organización de forma que se dé a conocer hacia el público en general.

5.3.1.5. Estrategia de introducción al mercado. Una vez se realiza la comercialización del producto se requiere asegurar que los usuarios lo utilicen de la manera correcta, para esto se definen las siguientes acciones acordadas en la reunión con los colaboradores del departamento de TI que se muestra en el Apéndice N. Minutas de Reuniones con la Organización. – Tabla N17.

- **Verificaciones:** Los sistemas de la organización permiten realizar un debido monitoreo de la aplicación de los controles como lo pueden las actualizaciones pendientes, alertas de seguridad, uso de la autenticación de múltiples factores por parte de usuarios y establecer políticas por grupos de usuarios que permitan garantizar el uso adecuado del SGSI.
- **Capacitaciones:** Para garantizar que los colaboradores del departamento de TI logren una adecuada implementación de los controles y su respectiva verificación se establece la necesidad de realizar las capacitaciones correspondientes.
- **Entrenamiento:** A partir de simulaciones de *phishing* y campañas de concientización se pretende que los colaboradores de la organización comprendan la importancia de aplicar los controles adecuados en la seguridad de la información y la manera correcta en que se debe utilizar el SGSI.
- **Evaluaciones:** Tanto antes como después de los entrenamientos y la concientización se estarán aplicando diferentes evaluaciones que permitan determinar el conocimiento adquirido por los colaboradores en la importancia y adecuada gestión de la seguridad de la información.

5.3.1.6. Conclusiones del Estudio de Mercado. A continuación se presentan las conclusiones obtenidas del estudio.

- A partir de los datos obtenidos tanto de fuentes primarias como secundarias se logra determinar que existe una demanda insatisfecha que requiere de la implementación del proyecto para obtener la certificación en el proceso de gestión de la seguridad de la información.
- La opción de oferta que puede ser más recomendable es INTECO por su localización y calidad garantizada de sus servicios, sin embargo se deben analizar los costos una vez recibidas todas las cotizaciones.
- La organización cuenta con las herramientas y recursos que le permiten establecer una adecuada estrategia para la comercialización.
- Es importante que los usuarios reciban las capacitaciones y entrenamientos necesarios que le permitan realizar un uso adecuado del SGSI.

5.3.2. Estudio Técnico

En el siguiente estudio se pretenden establecer los aspectos técnicos, estratégicos y de gestión necesarios para llevar a cabo el proyecto.

5.3.2.1. Objetivos Del Estudio. A continuación se presentan los objetivos planteados para el estudio técnico.

5.3.2.1.1. Objetivo General. A continuación se presenta el objetivo general del estudio técnico.

Definir los aspectos técnicos relacionados al tamaño, distribución y localización del proyecto para establecer las herramientas, información y recursos necesarios para la implementación del sistema de gestión de la seguridad de la información.

5.3.2.1.2. Objetivos Específicos. A continuación se definen los objetivos específicos del estudio técnico.

- Definir la localización óptima del proyecto.
- Analizar la disponibilidad y el costo de los suministros e insumos.
- Realizar la identificación y descripción del proceso.

5.3.2.2. Análisis de localización óptima del proyecto. En cuanto a la localización del proyecto se hace referencia a la infraestructura de TI en la organización sobre la cual se aplicarán los controles de seguridad detallados por el SGSI con la flexibilidad necesaria para satisfacer las necesidades específicas de los procesos de negocio.

Actualmente la empresa cuenta con una infraestructura de TI debidamente establecida para conseguir un funcionamiento efectivo del SGSI en todo su alcance. Dentro de los componentes que se toman en cuenta para analizar la localización del SGSI están los siguientes.

Tabla 33 *Componentes de la Infraestructura de TI*

Característica	Descripción
Proveedor de servicio de internet.	La organización cuenta con una conexión a internet primaria y una red secundaria como medida de contingencia ante eventualidades o fallos en la conexión.
Data Center.	La organización mantiene un data center en condiciones óptimas y con la seguridad tanto lógica como física necesaria.
Servidores.	Se cuenta con servidor firewall para el control de tráfico de información y comunicaciones además de los servidores de datos protegidos en el data center.
Cableado.	Las conexiones físicas a través del cableado se mantienen con la protección y la ubicación adecuada para mantener su seguridad.
Router y switch.	La organización cuenta con los equipos y la tecnología

Característica	Descripción
	necesaria para mantener las conexiones y redes locales seguras.
Puntos de acceso.	Se cuentan con los dispositivos para mantener la conexión inalámbrica estable entre los dispositivos y las áreas de trabajo.
Ancho de banda.	Se cuenta con un ancho de banda de 200 Mb/s en su red primaria y 20 Mb/s en su red secundaria.
Unidad NAS.	Se cuenta con una unidad de almacenamiento en red ubicada en el data center para mantener la recuperación centralizada de datos.
Computadoras.	Dentro de los activos de la organización se cuenta con computadoras tanto de escritorio como portátiles con componentes actualizados y capacitados para soportar la implementación adecuada de los controles de seguridad especificados por el SGSI.
Firewall.	Se mantienen controles de tráfico de la información en el dominio y fuera de este a través del firewall con reglas y protocolos definidos.
Seguridad.	Se mantienen los controles de acceso tanto físicos como lógicos debidamente implementados y verificados para garantizar la seguridad en la infraestructura de red.

La organización cuenta con la capacidad instalada suficiente para aplicar los controles en seguridad adecuados a la situación actual de la empresa, sin embargo se debe analizar si es necesario adquirir infraestructura como servicio para un nuevo servidor que cuente con las características específicas que sean requeridas para contar con la redundancia de la información que se determine como crítica, así como evaluar la necesidad de adquirir una licencia de antivirus que brinde la encriptación de información requerida.

5.3.2.3. Análisis del tamaño óptimo del proyecto. Para definir el tamaño óptimo del proyecto es fundamental identificar los requerimientos basado en las brechas que serán atacadas, según la priorización establecida en la **Tabla 29** del capítulo IV de este documento, de forma que se pueda conseguir un producto que abarque las principales necesidades

presentadas en los controles de las áreas con un nivel de cumplimiento menor al 85%. Con esto se pretende definir la complejidad de la solución y componentes necesarios para su desarrollo.

En la siguiente **Tabla 34** se muestra la lista de los requerimientos organizacionales necesarios de integrar en el SGSI.

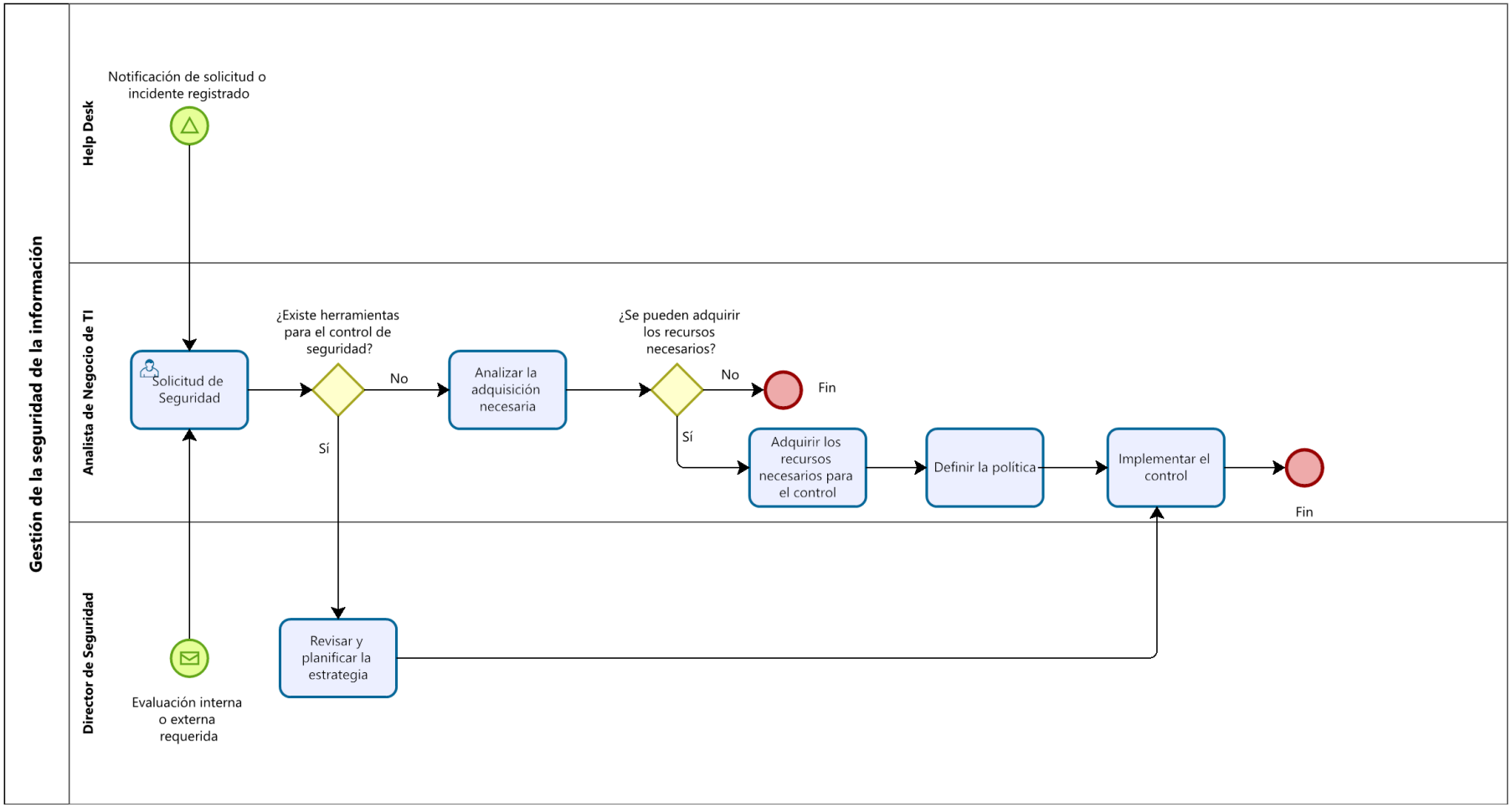
Tabla 34. *Requerimientos organizacionales para atender las brechas identificadas.*

ID	Requerimiento
RO-01	El sistema requiere de la implementación de un proceso para la gestión de riesgos debidamente documentado y aprobado por los responsables.
RO-02	El sistema requiere incluir una política establecida en la relación con proveedores que especifique la cadena de suministro de tecnologías de información y comunicación.
RO-03	Se deben establecer políticas que permitan la adecuada gestión de cambios en los servicios con proveedores.
RO-04	Se requiere implementar controles para el adecuado etiquetado y clasificación de la información.
RO-05	Se deben implementar políticas para la correcta eliminación, transporte y gestión de medios extraíbles que respondan a las brechas encontradas en el proceso de gestión de activos.
RO-06	Se requiere establecer y documentar la información, acciones y responsables del contacto con las autoridades pertinentes a las cuales recurrir ante un incidente de seguridad de la información.
RO-07	Se deben implementar controles para encriptar los datos en los equipos faltantes (computadoras de escritorio y servidores) y asegurar su cumplimiento.
RO-08	Se debe mejorar el método para la correcta gestión de claves a través de herramientas que garanticen su seguridad.
RO-09	Se debe incluir los riesgos relacionados con terceras partes en el proceso de gestión de riesgos.
RO-10	Se requiere establecer una política para la gestión de servicios en la nube.
RO-11	Se deben establecer políticas para determinar la información crítica que requiere la redundancia de disponibilidad.

5.3.2.4. Identificación y descripción del proceso. El proyecto consiste en alinear el sistema de gestión de la seguridad de la información con la norma ISO 27001:2013, el cual permita al Departamento de TI prepararse para optar por la respectiva certificación.

Actualmente el proceso de gestión de seguridad de la información se encuentra en una etapa inicial como se muestra en la siguiente **Figura 8** que muestra el diagrama As-Is del proceso, obtenido a partir de la reunión con la Analista de Negocio de TI y el Analista de Negocio CRM del Departamento de TI (ver Apéndice N. Minutas de Reuniones con la Organización. – Tabla N20).

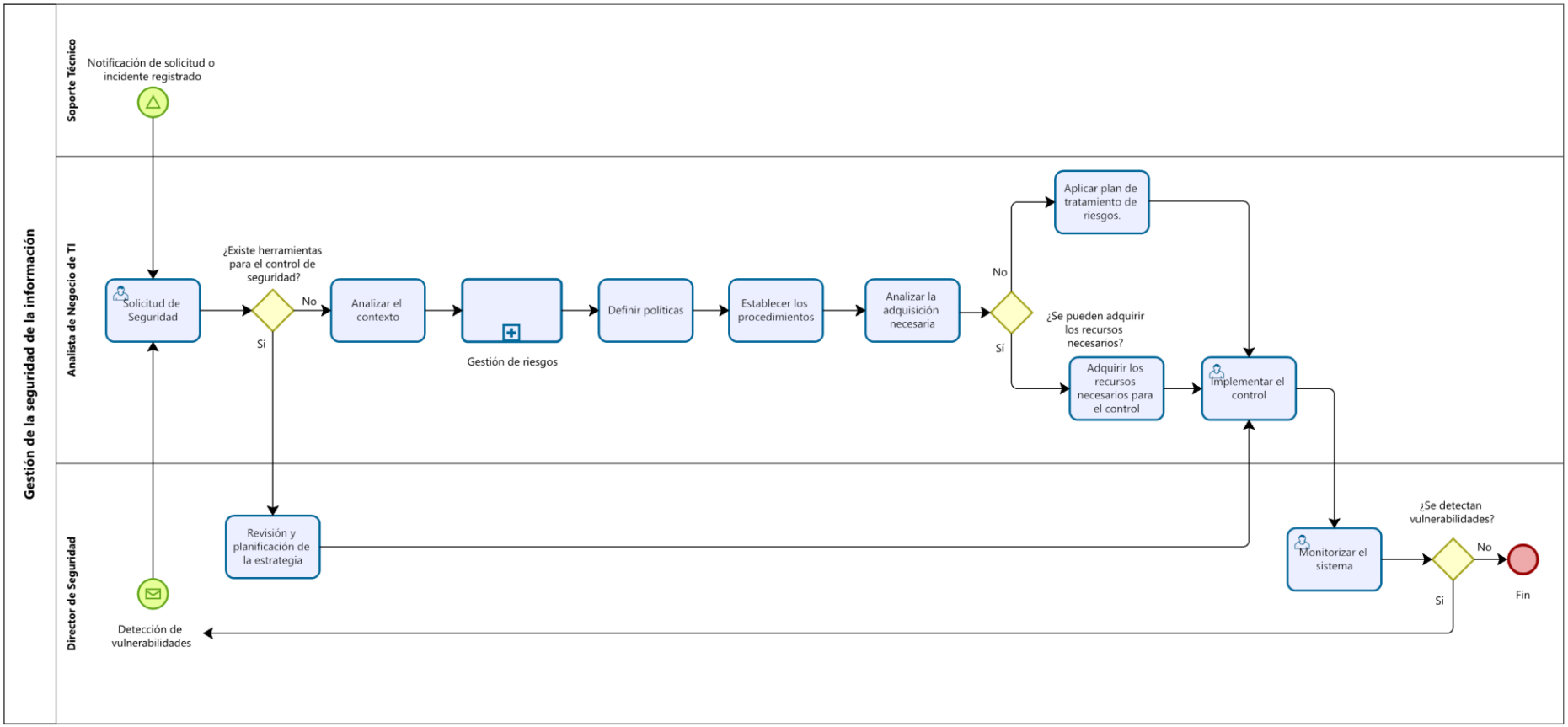
***Figura 8**. Diagrama As-Is del Proceso de Gestión de la Seguridad de la Información.*



La principal necesidad que se observa en el proceso actual es la definición e implementación del proceso de gestión de riesgos que permita identificar, evaluar y tratar adecuadamente los riesgos en seguridad de la información que podría presentar la organización.

Al implementar la propuesta planteada se pretende obtener la mejora en el proceso de gestión de la seguridad de la información que se muestra en la **Figura 9.** Diagrama To-Be del Proceso de Gestión de Seguridad d la Información el diagrama To-Be esperado.

Figura 9. *Diagrama To-Be del Proceso de Gestión de Seguridad d la Información*



El proceso de gestión de riesgos establecido como subproceso en el diagrama anterior se define en la siguiente sección de este documento.

Para atender las brechas encontradas se propone a la organización establecer los procesos y controles que requieren ser implementados, además de definir las actualizaciones necesarias a la política de seguridad de la información. A continuación se describen los procesos a implementar y las actualizaciones a la política interna propuestos.

5.3.2.5. Procesos a implementar. En esta sección se detallan los procesos y controles que requieren ser implementados en la organización.

5.3.2.5.1. Gestión de Riesgos. Al presentar una ausencia del proceso para la gestión de riesgos se proponen las siguientes acciones que permitan realizar la adecuada definición e implementación del proceso.

Para definir el proceso se necesita contar con los siguientes recursos humanos.

- **Ingeniero de Procesos:** se requiere definir un encargado de gestionar los riesgos periódicamente a través del proceso definido a continuación.
- **Director de Seguridad:** Revisión mensual durante el primer año en el que se implementa el proceso de forma que se mantenga una monitorización constante que evalúe la correcta adaptación del proceso en el Departamento de TI.

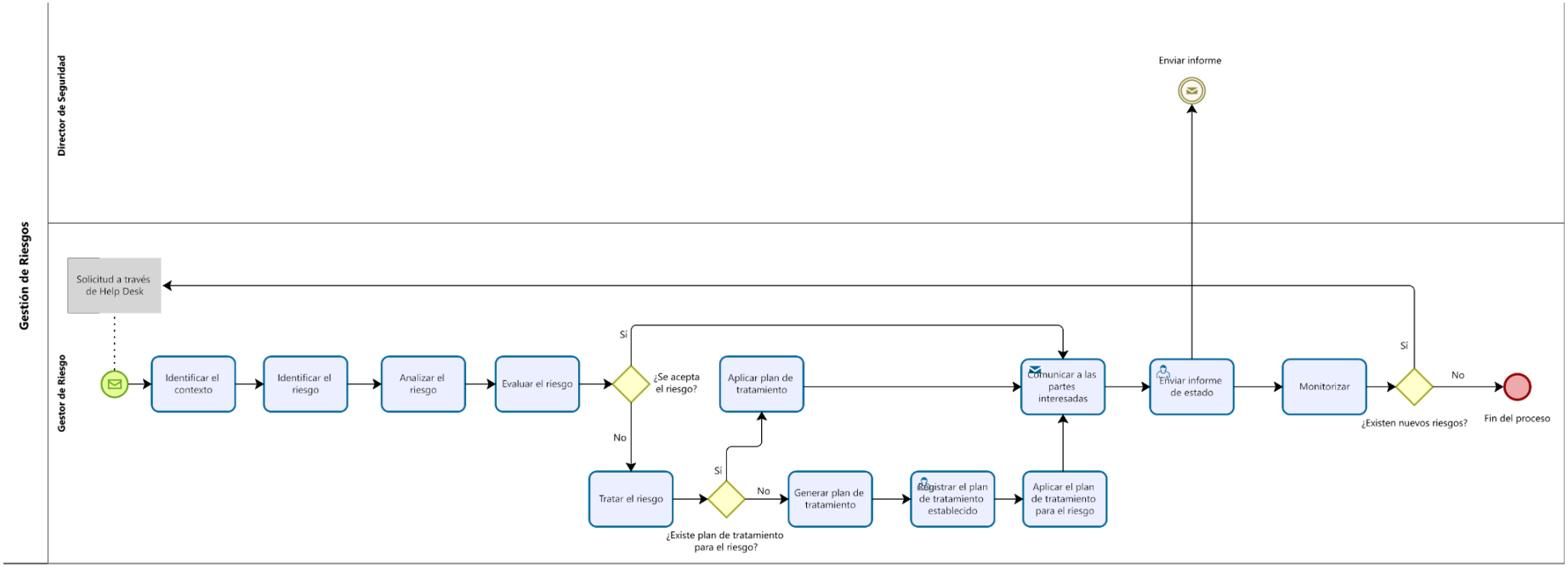
Se pretende que la matriz de evaluación de la seguridad de la información desarrollada en este proyecto sea el insumo que permita definir el proceso para contar posteriormente con la matriz de evaluación de riesgos como se muestra en la siguiente **Tabla 35.** Entradas y Salidas del Proceso de Gestión de Riesgos.

Tabla 35. *Entradas y Salidas del Proceso de Gestión de Riesgos*

Entradas	Proceso	Salidas
Matriz de evaluación de seguridad de la información	Gestión de riesgos	Matriz de evaluación de riesgos

Al no contar con un proceso de gestión de riesgos previo que permitiera definir un modelo As-Is se establece únicamente la siguiente propuesta del proceso en el diagrama To-Be que se presenta en la **Figura 11**.

Figura 10 Diagrama To-Be del Proceso de Gestión de Riesgos.



En el diagrama de flujo mostrado anteriormente se muestra la propuesta del proceso para la adecuada gestión del riesgo, el cual está basado en la norma ISO 31000:2018, que establece los subprocesos necesarios para su respectiva implementación.

5.3.2.5.2. Gestión de activos. Actualmente la organización cuenta con un proceso definido para gestión de activos a cargo del analista de negocio, sin embargo se identifica la ausencia de controles que permitan realizar una adecuada clasificación y etiquetado de los activos de información. Por esta razón se presenta la siguiente propuesta de clasificación alineada a ISO 27001:2013.

5.3.2.5.2.1. Clasificación de activos de información. A falta de una respectiva clasificación de los activos de información que brinde la protección adecuada según niveles de acceso a partir de su criticidad se propone a la organización implementar la siguiente clasificación de acuerdo con los principios de la seguridad de la información los cuales son: confidencialidad, integridad y disponibilidad; de forma que se cumpla con lo estipulado por las normas ISO 27001:2013 e ISO 27002:2013.

Para esta clasificación se identifican los siguientes tipos de activos de información de la organización.

- Información física
- Información digital
- Hardware
- Software
- Personas

Para realizar una adecuada clasificación se toman en cuenta los criterios de confidencialidad, integridad y disponibilidad de la información.

I. **Clasificación de acuerdo a la confidencialidad:** Para esta clasificación se proponen las siguientes categorías presentadas en la **Tabla 36** establecidas a partir de la reunión con el Analista de Negocio de TI y Analista de Negocio CRM (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N20).

Tabla 36. *Clasificación de acuerdo con la confidencialidad de la información.*

Clasificación	Descripción
Confidencial (C)	Toda aquella información que debe estar disponible únicamente para conocimiento de los procesos internos de la organización y que puede generar un impacto negativo si es revelada a terceros. Se incluye toda información personal y datos de los clientes de la organización que requieren manejarse confidencialmente.
Interna/Privada (I)	Información de conocimiento general dentro de la organización que requiere de autorización de su responsable para ser revelada a terceros.
Pública (P)	Información conocida tanto de forma interna como externa de la organización la cual no representa riesgos para la organización.
No clasificada	Todos aquellos activos de información que no se encuentren clasificados deberían tratarse como: Confidencial.

II. **Clasificación de acuerdo con la integridad:** Para esta clasificación se proponen las siguientes categorías presentadas en la **Tabla 37** establecidas a partir de la reunión con el Analista de Negocio de TI y Analista de Negocio CRM (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N20).

Tabla 37. *Clasificación de Acuerdo con la Integridad de la Información*

Clasificación	Descripción
Alta	Información que se requiere mantener precisa y completa para evitar impactos altamente negativos que generen graves consecuencias a la organización.
Media	Información que se requiere mantener precisa y completa para evitar impactos negativos que puedan generar algunas consecuencias a la organización.
Baja	Información que no representa un impacto significativo y no es necesario mantener su precisión y exactitud.
No clasificada	Todos aquellos activos de información que no se encuentren clasificados deberían tratarse como: Alta integridad.

III. **Clasificación de acuerdo con la disponibilidad:** Para esta clasificación se proponen las siguientes categorías presentadas en la **Tabla 38** establecidas a partir de la reunión con el Analista de Negocio de TI y Analista de Negocio CRM (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N20).

Tabla 38. *Clasificación de Acuerdo con la Disponibilidad de la Información.*

Clasificación	Descripción
Alta	La ausencia de disponibilidad en la información genera impactos altamente negativos que provocan graves consecuencias a la organización.
Media	La ausencia de disponibilidad en la información genera impactos que podrían provocar algunas consecuencias a la organización.
Baja	La ausencia de disponibilidad en la información no representa un impacto significativo para la organización.

Clasificación	Descripción
No clasificada	Todos aquellos activos de información que no se encuentren clasificados deberían tratarse con: Alta disponibilidad.

Tomando como referencia los criterios de clasificación mencionados anteriormente se establece la siguiente propuesta para el etiquetado de la información.

5.3.2.5.2.1. Etiquetado de los activos de información: Para realizar el etiquetado de los activos de información se establecen los siguientes aspectos por tomar en cuenta.

- Se deben etiquetar todos los activos que se encuentren clasificados según lo establecido en el apartado **Clasificación de activos de información.**
- La etiqueta del activo debe incluir la identificación según los niveles de confidencialidad, integridad y disponibilidad.
- Cualquier activo no etiquetado debe ser tratado en la categoría de “No clasificada” en todos los criterios (confidencialidad, integridad y disponibilidad).
- Se deben utilizar los siguientes identificadores para cada etiqueta según su clasificación en los criterios de confidencialidad, integridad y disponibilidad como se muestra en la **Tabla 39**.

Tabla 39. *Nomenclatura Para el Etiquetado de la Información.*

Confidencialidad	Integridad	Disponibilidad
Confidencial = C	Alta = A	Alta = 3
Interna = I	Media = M	Media = 2
Pública = P	Baja = B	Baja = 1

- Todo activo debe contener en su etiqueta un código que identifique su nivel de confidencialidad, integridad y disponibilidad (en adelante llamado código CID) de acuerdo con lo establecido en la **Tabla 39**, de forma que los activos físicos lo

muestren en su etiqueta de identificación y los activos digitales en el nombre de los archivos, como lo muestran las **Figura 11.** Código CID Para el Etiquetado de Activos Físicos y **Figura 12.** Código CID Para el Etiquetado de Activos Digitales.

Figura 11. *Código CID Para el Etiquetado de Activos Físicos*

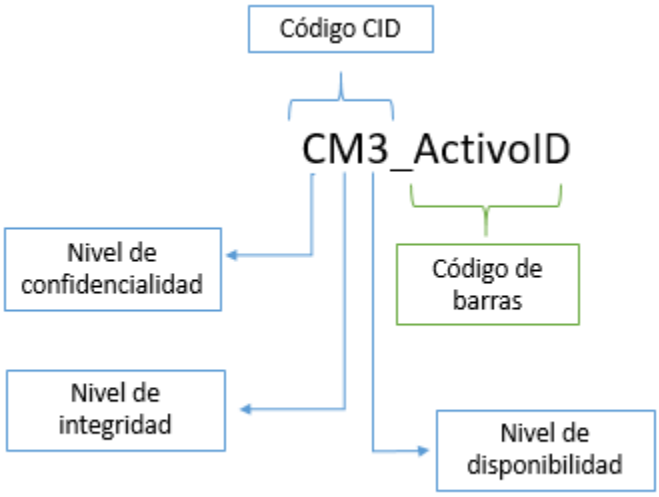
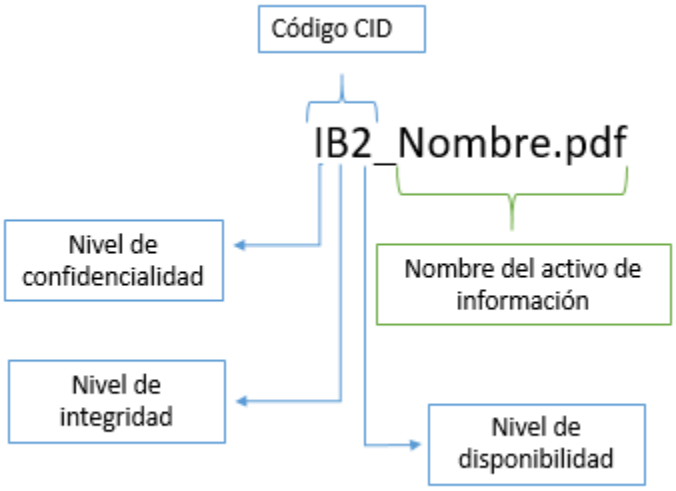


Figura 12. *Código CID Para el Etiquetado de Activos Digitales.*



Se recomienda que la organización realice la actualización de la clasificación de un activo en el momento que haya una reasignación o daño del activo.

5.3.2.6. Actualizaciones de la Política de Seguridad de la Información. Según las brechas encontradas se requiere la implementación de políticas y controles, los cuales deben ser establecidos por la organización.

A continuación se especifican las áreas y se proponen los objetivos que deben ser contemplados para definir dichas políticas y controles según lo establecido por la International Organization for Standardization (2013b).

I. ***Cadena de suministro de tecnología de información y de las comunicaciones.*** Para definir las políticas, controles y procedimientos en relación con la cadena de suministro de las tecnologías de información y comunicación (TIC), se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 15.2.2 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. - Apartado: G.1).

II. ***Gestión de cambios en servicios con proveedores*****.** Para definir las políticas, controles y procedimientos en relación con la gestión de cambios en servicios con proveedores, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 15.1.3 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos.– Apartado: G.2).

III. ***Clasificación de la información.*** Para definir las políticas, controles y procedimientos en relación con la clasificación de la información, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 8.1.2 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía

de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.3).

IV. ***Etiquetado de la información.*** Para definir las políticas, controles y procedimientos en relación con el etiquetado de la información, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 8.2.2 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.4).

V. ***Gestión de medios extraíbles.*** Para definir las políticas, controles y procedimientos en relación con la gestión de medios extraíbles, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 8.3.1 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.5).

VI. ***Eliminación de medios extraíbles.*** Para definir las políticas, controles y procedimientos en relación con la eliminación de medios extraíbles, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 8.3.2 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.6).

VII. ***Transporte de medios extraíbles.*** Para definir las políticas, controles y procedimientos en relación con el transporte de medios extraíbles, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 8.3.3 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.7).

VIII. ***Contacto con las autoridades.*** Para definir las políticas, controles y procedimientos relacionados al contacto con autoridades pertinentes, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 6.1.3 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.8).

IX. ***Política en el uso de controles criptográficos.*** Para definir las políticas, controles y procedimientos relacionados al uso de controles criptográficos, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 10.1.1 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.9).

X. ***Gestión de claves.*** Para definir las políticas, controles y procedimientos relacionados con la gestión de claves, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 10.1.2 de la norma ISO 27002:2013 que establece los controles y aspectos por tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.10).

XI. ***Disponibilidad de los recursos de tratamiento de la información.*** Para definir las políticas, controles y procedimientos relacionados con la redundancia y disponibilidad de los recursos de tratamiento, se recomienda que el encargado de llevar a cabo el proceso tome como referencia el apartado 17.2.1 de la norma ISO 27002:2013 que establece los controles y aspectos a tomar en cuenta en su guía de cumplimiento (ver Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos. – Apartado: G.11).

XII. ***Tercerización.*** Los controles y políticas que se necesitan implementar en la organización se abarcan en la sección de gestión de proveedores y se deben incluir los riesgos asociados a esta área en el proceso de gestión de riesgos pendiente de definir por la organización.

XIII. ***Servicios en la nube.*** Las brechas encontradas en el área de servicios en la nube no serán tomadas en cuenta para el alcance de esta propuesta debido a que la organización cuenta con un practicante de la carrera de ATI encargado de definir el proceso.

5.3.2.7. Mejora continua. Para establecer y gestionar adecuadamente el SGSI se requiere implementar el proceso cíclico de Deming que presenta cuatro pasos para la mejora continua del sistema: planificar, hacer, verificar y actuar (PHVA).

Este ciclo de mejora continua permite a la organización brindar la monitorización y actualización del sistema al identificar, a través de las auditorías internas y externas, las políticas y controles que requieren implementarse para atender las necesidades de los clientes y los requerimientos de la organización.

Una vez se implementen las acciones propuestas para atacar las principales brechas, según lo establecido en la sección 5.3.2.5. Procesos a implementar y la sección 5.3.2.6. Actualizaciones de la Política de Seguridad de la Información, del presente Estudio Técnico, se espera que a través de esta metodología la organización mantenga una constante evaluación que permita atender las áreas que cuentan con un nivel de capacidad de “Completamente” para garantizar la mejora continua del SGSI.

Los pasos para garantizar la mejora continua del sistema se mencionan a continuación.

5.3.2.7.1. Planificar. Como primer paso es necesaria una contextualización de la situación actual en la que se encuentra la organización.

Para ello es necesario evaluar factores tanto internos como externos de la organización en materia de seguridad de la información, analizando las demandas de la industria y los requerimientos de los clientes, así como los objetivos planteados por la empresa y el Departamento de TI.

A partir de los resultados obtenidos en la matriz “Evaluación de la Seguridad de la Información”, definida y adjuntada en el Apéndice G, las observaciones y comentarios expresados por los colaboradores y el análisis a los cuestionarios enviados por los clientes, se podrán establecer los requerimientos, objetivos, alcance, procesos, políticas y procedimientos en materia de seguridad de la información que permitan gestionar adecuadamente los riesgos asociados para cumplir con los objetivos y políticas de la organización a través de la implementación del SGSI a lo largo del tiempo.

5.3.2.7.2. Hacer. Una vez se tiene claro el contexto se deben establecer las políticas y procedimientos adecuados a la organización e implementar los controles que el sistema de gestión de seguridad de la información debe contener para garantizar el cumplimiento de su objetivo y la adecuada aplicación de las políticas y procedimientos establecidos en sus diferentes áreas de control en la organización.

Debido a las limitaciones presentadas en los recursos humanos del Departamento de TI y la disponibilidad de tiempo necesario para llevar a cabo la implementación de dichos procedimientos, se recomienda la contratación de personal capacitado responsable de definir e implementar los procesos requeridos por el SGSI.

5.3.2.7.3. Verificar. A través de las auditorías internas y externas se debe mantener la evaluación periódica que permita medir el desempeño del SGSI y brindar los reportes de los resultados a responsables y directivos para que puedan establecer las acciones a tomar y las actualizaciones correspondientes del sistema.

Estas auditorías verificarán la respectiva documentación de las políticas y controles así como la adecuada ejecución de los procedimientos establecidos para cada control.

Dentro de los hallazgos se identifica que la organización no cuenta con personal formado en auditoría y los procesos de auditoria interna se realizan de manera informal y únicamente cuando se deben hacer mejoras o actualizaciones en procesos determinados.

Para llevar a cabo el proceso de verificación es fundamental que la organización tome en cuenta las siguientes necesidades identificadas.

- Capacitar un responsable certificado en auditoría que asuma el rol de auditor interno, el cual pueda de llevar a cabo las respectivas verificaciones del cumplimiento de los procedimientos.
- Establecer proceso paulatino de desarrollo de auditoría interna que se encuentre alineado a la cultura organizacional.
- Definir los mecanismos de coordinación para destinar los recursos necesarios que permitan implementar las mejoras y actualizaciones identificadas en la auditoría.

5.3.2.7.4. Actuar. Para asegurar el correcto funcionamiento del sistema se requiere de constantes acciones correctivas y preventivas que permitan establecer las mejoras a implementar en el SGSI basado en los resultados de las auditorías, de forma que se atiendan las necesidades de la organización y nuevos requerimientos por parte de los clientes.

Los resultados obtenidos serán registrados en la Matriz de Evaluación de Seguridad de la Información (ver Apéndice H. Matriz de Evaluación de la Seguridad de la Información.) de forma que se mantenga actualizada y sea la herramienta que permita conocer el estado actual del SGSI.

Estas actualizaciones deben ser comunicadas adecuadamente a las partes interesadas a través del correo electrónico interno y su respectiva publicación en Microsoft SharePoint de forma que se logren obtener los resultados esperados de en todas las áreas de la organización.

5.3.2.8. Disponibilidad y costo de los insumos. Para tomar acción de los diferentes requerimientos organizacionales presentados en la **Tabla 34**, se deben establecer diferentes procesos, los cuales requieren de estudios correspondientes que demandan como principal recurso el tiempo de trabajo de los colaboradores a cargo de definir dichos procesos.

Al llevar a cabo las actividades que permitan atacar las principales brechas identificadas es importante tomar en cuenta lo mencionado por Baca Urbina (2016), el cual se refiere a la mano de obra directa como aquellos recursos humanos encargados del desarrollo, para el presente caso corresponden a los encargados de desarrollar los procesos y políticas necesarias para solventar las brechas identificadas, así como la mano de obra indirecta que serán los responsables de la verificación y aprobación de los procesos, además de los encargados del monitoreo posterior a la implementación.

En la siguiente **Tabla 40** se muestran los recursos humanos necesarios para el proyecto.

Tabla 40. *Recursos Humanos Necesarios.*

Mano de Obra Directa	Mano de Obra Indirecta
• Analista de Negocio de TI • Analista de Negocio CRM	• Director de Seguridad

Mano de Obra Directa	Mano de Obra Indirecta
• Ingeniero de Procesos • Auditor Interno	

Debido a lo anterior se establece, en la siguiente **Tabla 41** las estimaciones del tiempo que podrían tomar cada una de las tareas y el costo que representa según las horas laborales.

Para determinar la estimación del costo se toma como referencia el costo promedio por hora laboral correspondiente a $31, así como los tiempos que estima el Departamento de TI para la duración de cada actividad. Estos datos fueron brindados por la Analista de Negocio de TI (ver Apéndice N. Minutas de Reuniones con la Organización. - Tabla N23).

Tabla 41. *Actividades a Ejecutar Para Cerrar las Brechas Identificadas.*

Actividad	Tiempo Estimado	Costo Estimado
Establecer e implementar el proceso de gestión de riesgos	192h	$5,952
Definir las políticas y mejoras necesarias en el proceso de gestión de proveedores.	30h	$930
Definir los controles y políticas necesarias para la gestión de activos.	52h	$1,612
Definir los criterios para la encriptación.	5h	$155
Definir políticas para la redundancia de la disponibilidad de la información	5h	$155
Capacitaciones	24h	$744
Monitorización	48h	$1,488
Auditoría interna	24h	$744

5.3.2.9. Posibles inversiones adicionales del proyecto. Para que la organización pueda cumplir con los diferentes controles y requerimientos del sistema se requieren de estudios previos que determinen si la capacidad de los equipos con que cuenta la infraestructura

actualmente es suficiente para soportar la implementación de los controles y las acciones de mejora.

Por esta razón se establecen algunos de los equipos y dispositivos que deberían ser evaluados así como su respectiva estimación del costo que representaría en caso de ser necesaria su adquisición.

- Servidor en la nube
- Licencia ESET Protect Complete

De acuerdo con las limitaciones que pueda presentar el centro de datos de la organización se determina que la opción más atractiva para la empresa es contratar infraestructura como servicio para adquirir un servidor en nube privada, el cual brinde la capacidad de redundancia y la seguridad de la información necesarias para garantizar los controles que se requieren implementar.

El departamento de TI solicitó la respectiva cotización del servidor con las características y requerimientos específicos, los cuales no son mencionados en este documento para resguardo de la confidencialidad. Sin embargo, es importante recalcar que el centro de datos donde se ubica el servidor cuenta con certificaciones en ISO 27001 y Tier III, además de ofrecer la capacidad necesaria para atender las brechas en redundancia de la información presentadas.

Para el caso de la licencia de antivirus se realiza una estimación del costo anual para cien equipos de acuerdo con los datos proporcionados por la página oficial Protect Complete (2021).

Las respectivas estimaciones de costo serán detalladas en el análisis financiero realizado en este documento.

5.3.2.10. Determinar la organización humana y jurídica necesaria para el desarrollo de las diferentes actividades requeridas por el sistema se debe tomar en cuenta las estimaciones realizadas en la duración y recursos humanos necesarios que se presentaron en la sección **5.3.2.8. Disponibilidad y costo de los insumos** de forma que sea posible determinar si existen colaboradores con la suficiente disponibilidad para asumir las diferentes tareas y definir los procesos y políticas necesarias.

Para esto se definen los posibles escenarios que se muestran a continuación.

- **Reestructuración del departamento de TI:** una posible opción es realizar una reestructuración de las responsabilidades en el departamento de forma que se puedan asignar procesos por definir y trabajar de forma paralela en atender diferentes requerimientos del sistema.

  Se deben tomar en cuenta las limitaciones que se pueden presentar en la carga de trabajo de los colaboradores del departamento y evaluar las capacitaciones necesarias en el personal a cargo de definir e implementar los procesos y políticas.

  Contratación: En caso que las limitaciones en el recurso humano no permitan la asignación de responsables para definir e implementar los procesos y políticas necesarios, se propone evaluar la posibilidad de realizar la contratación de personal calificado que brinde el apoyo para llevar a cabo la definición de los procesos y controles necesarios.

  En la siguiente **Tabla 42** se definen algunos de los aspectos por tomar en cuenta en el perfil de contratación.

***Tabla 42**. Perfil del Puesto a Contratar.*

Perfil	Descripción
Puesto	Ingeniero de Procesos
Estudios	Graduado en ciencias informáticas o tecnologías de información
Nivel	Junior
Responsabilidades	• Analizar y comprender el contexto de la organización y los procesos de negocio. • Definir e implementar mejoras en los procesos de negocio y sistemas. • Brindar soporte en las operaciones del departamento. • Elaboración de presupuestos y análisis de mercado.
Conocimientos y competencias	• Capacidad para la resolución de problemas. • Gestión de recursos, tiempo, calidad, alcance y riesgos. • Conocimiento en certificaciones. • Conocimiento en procesos de negocios • Conocimiento en metodologías ágiles y buenas prácticas.

5.3.2.11. Legislación relevante. Es importante que la organización tenga presente algunas leyes relacionadas con la seguridad de la información que permitan mantener el sistema alineado a la legislación establecida por el país en el que opera.

En la siguiente **Tabla 43** se detallan las leyes y una breve descripción de su enfoque y relevancia para el sistema.

***Tabla 43.** Leyes Relevantes a Tomar en Consideración*

Ley	Descripción
Ley Nº 8968: Protección de la Persona frente al tratamiento de sus datos personales.	Especifica las reglas generales en el adecuado tratamiento de los datos personales y la protección de la información sensible.
Ley N° 9048: Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.	Reformas y adiciones al código penal que incluyen acciones en contra de los delitos informáticos.

Ley	Descripción
Ley 8148: Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos.	
Ley Nº 8454: Certificados, Firmas Digitales y Documentos Electrónicos	Establece las regulaciones para la documentación legal que requiera certificación o firmas digitales.
Ley N° 7975: Información No Divulgada	Enfocada en la protección de la información relacionada con secretos comerciales y de carácter crítico para las organizaciones.

En la siguiente **Tabla 44** se muestran los decretos emitidos relevantes para el proyecto.

***Tabla 44**. Decretos Relevantes a Tomar en Consideración*

Decreto	Descripción
Nº 37052-MICIT: Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR	Apoyo a empresas tanto públicas como privadas en la prevención y respuesta ante incidentes relacionados con la seguridad de la información que afecten a instituciones gubernamentales.

Existe un convenio internacional contra delitos informáticos que debería ser considerado como se muestra en la **Tabla 45**.

***Tabla 45**. Convenio Relevante a Tomar en Consideración*

Convenio	Descripción
Convenio de Budapest	Tratado internacional que establece una política penal contra delitos informáticos.

5.3.3. Gestión de riesgos

Realizar un estudio de riesgos es vital al momento de definir un sistema de gestión de seguridad de la información, de manera que sea posible identificar aquellos aspectos que pueden afectar la capacidad para conseguir los objetivos del sistema.

Para el análisis de los riesgos se requiere identificar los principales activos de información por su tipo de forma que sea posible determinar las posibles amenazas, vulnerabilidades y consecuencias que podrían presentarse. De esta forma será posible determinar los riesgos relacionados con las brechas que deben ser atacadas como parte de la propuesta.

Se entienden por riesgos en seguridad de la información como aquellos aspectos que deben ser evitados por la organización debido a su generación de amenazas o al bloqueo para conseguir oportunidades identificadas (ITIL, 2011).

Existen algunos tipos de riesgos que pueden incluir categorías como riesgos de: reputación, financieros, legales, estratégicos, producción y seguridad. Para efectos de este proyecto se identifican los riesgos relacionados con la seguridad de la información que pueden representar amenazas en la organización que impidan el objetivo planteado.

Para realizar una adecuada identificación se toma como referencia lo establecido por la norma ISO 27005:2018 de forma que se mantenga la alineación con el estándar.

En la siguiente **Tabla 46** se identifican los activos de información en la organización y se clasifican según su tipo.

Tabla 46 *Activos de Información*

Clasificación	Activos de información
Información digital	Repositorio
	Correos electrónicos
	Bases de datos
	Copias de seguridad

Clasificación	Activos de información
	Código fuente
Información física	Políticas internas
	Contratos
Software	Licencias
	Cortafuegos
	Aplicaciones
Hardware	Servidores
	Computadoras
	Medios extraíbles
Personas	Empleados
	Subcontratados

5.3.3.1. Identificación de Amenazas, Vulnerabilidades y Consecuencias. La organización cuenta con licencias de Microsoft para las herramientas SharePoint, Azure DevOps Server, Active Directory y Office 365 en las que almacena y comparte toda la información interna, además de contener los medios para la respectiva comunicación.

La organización cuenta con un centro de datos en el que almacena múltiples servidores y unidades de almacenamiento, además cada departamento y colaborador cuenta con su respectiva computadora de escritorio y laptops para el desarrollo de las funciones diarias. Además se tienen medios de almacenamiento extraíbles como discos duros y memorias USB para el transporte y almacenamiento de información.

En la siguiente **Tabla 47** se muestran las amenazas, vulnerabilidades y consecuencias identificadas de acuerdo con las brechas encontradas en las diferentes áreas de la matriz de evaluación de la seguridad de la información y los activos con los que cuenta la organización.

Tabla 47. *Amenazas, Vulnerabilidades y Posibles Consecuencias Identificadas.*

Amenazas	Vulnerabilidades	Posibles consecuencias
• Phishing • Ataques DoS. • Problemas en el servicio de internet. • Modificación o eliminación de datos no autorizados. • Deterioro o pérdida de documentos. • Robo de información. • Acceso no autorizado a información sensible. • Deterioro físico de los equipos. • Robo del dispositivo. .	• No se cuenta con un proceso definido ni implementado para la gestión de riesgos. • No se cuentan con controles para garantizar la redundancia en la disponibilidad de la información. • No se cuenta con la respectiva segregación de las redes. • No se realizan revisiones de los derechos de acceso. • No se identifica la información crítica a respaldar. • No se cuentan con controles para garantizar la redundancia en la disponibilidad de la información crítica. • No se cuentan con controles para la seguridad de la información en medios extraíbles. • No se realizan entrenamientos, capacitaciones y concientización en seguridad de la información de forma periódica.	• Materialización de los riesgos sin un plan para mitigarlos. • No contar con la información disponible en el momento requerido. • Acceso no autorizado a datos sensibles de la organización. • Robo de información sensible. • No contar con la información disponible en el momento requerido. • Daños en hardware provocados por software malicioso. • Pérdida de información por error humano.

5.3.3.2. Riesgos Identificados. A continuación se muestran los diferentes riesgos identificados según las amenazas, vulnerabilidades y consecuencias definidas anteriormente.

- Materialización de riesgos debido a la ausencia de un proceso de gestión de riesgo que permita identificar y mitigar dichos riesgos.
- Retrasos y problemas en la cadena de suministro de tecnología debido a la falta de una política.
- Errores en la ejecución y aumento de costos debido a la falta de políticas en la gestión de cambios con proveedores.
- Pérdida o robo de información sensible de la organización o clientes por falta de controles en la gestión de medios extraíbles.
- Robo de equipos debido al traslado de los colaboradores y el teletrabajo.
- Pérdida de información de los clientes o a nivel interno de la organización por ataques de software malicioso.
- Presencia de software malicioso en los equipos de los colaboradores ante la ausencia de herramientas para la protección de los equipos personales.
- Retrasos en operaciones y procesos por problemas en la red que generan problemas de disponibilidad de la información.
- Modificación o eliminación no autorizada de la información debido a la falta de revisión de los permisos de acceso.
- Instalación de malware por parte de colaboradores en los equipos debido a la falta de controles en la instalación de software.
- Vulnerabilidades generadas por la falta de conocimiento y concienciación en colaboradores sobre la seguridad de información.

5.3.3.3. Análisis de riesgos. Para identificar los diferentes riesgos asociados al SGSI se recurre al análisis cualitativo a través de una reunión con los colaboradores del departamento que se muestra en el anexo# en el cual se definen los niveles de probabilidad e impacto que se detallan a continuación.

5.3.3.3.1. Probabilidad. En la siguiente ***Tabla 48*** se definen los siguientes criterios para la evaluación de la probabilidad según lo acordado en reunión con los colaboradores del departamento (ver Apéndice N. Minutas de Reuniones con la Organización. – Tabla N24).

Tabla 48. *Niveles de Probabilidad de Riesgo*

Probabilidad	Descripción	Nivel de probabilidad
Inusual	Riesgos con probabilidad de ocurrir casi nula o no esperada.	1
Improbable	Riesgos con probabilidad baja de ocurrir	2
Posible	Riesgos con probabilidad esperada de ocurrir	3
Muy Probable	Riesgos con alta probabilidad de ocurrir	4
Frecuente	Riesgos con probabilidad de ocurrir casi siempre o periódicamente	5

5.3.3.3.2. Impacto. En la siguiente **Tabla 49** se definen los siguientes criterios para la evaluación del impacto según lo acordado en reunión con los colaboradores del departamento (ver Apéndice N. Minutas de Reuniones con la Organización. – Tabla N24).

Tabla 49. *Niveles de Impacto de Riesgos.*

Probabilidad	**Descripción**	**Nivel de Impacto**
Insignificante	Problemas operativos, existen algunos problemas de control interno, aunque se pueden solucionar de inmediato.	**1**
Menor	Problemas operativos, existen algunos problemas de control interno, pero no crean brechas de seguridad.	**2**

Moderado	Errores ocasionales continuos, incumplimiento de los controles internos y normativas legales.	**3**
Peligroso	Errores continuos significativos, incumplimiento de los controles internos y normativas legales.	**4**
Catastrófico	Impactos críticos, hay errores importantes o falta severa en el cumplimiento de las regulaciones de la empresa.	**5**

5.3.3.3.3. Niveles de Riesgo. Una vez se conforman los respectivos criterios para la evaluación de la probabilidad y el impacto, se establece la siguiente **Tabla 50** en la que se muestran los niveles de riesgo de acuerdo con las calificaciones otorgadas en la probabilidad y el impacto de cada riesgo.

Tabla 50. *Niveles de Riesgo.*

Niveles de Riesgo	
Probabilidad : Impacto	**Nivel de Riesgo**
1:1	Bajo
2:1	Bajo
3:1	Bajo
4:1	Bajo
1:2	Bajo
2:2	Bajo
1:3	Bajo
5:1	Medio
5:2	Medio
4:2	Medio
3:2	Medio
3:3	Medio
2:3	Medio
2:4	Medio

Niveles de Riesgo	
Probabilidad : Impacto	**Nivel de Riesgo**
1:4	Medio
1:5	Medio
5:3	Alto
4:3	Alto
5:4	Alto
4:4	Alto
3:4	Alto
5:5	Alto
4:5	Alto
3:5	Alto
2:5	Alto

5.3.3.4. Matriz de riesgos. La siguiente matriz de riesgos presentada en la **Tabla 51** se obtiene a partir de los riesgos identificados para la organización así como la asignación de su probabilidad e impacto. Esta valoración fue realizada en conjunto con los analistas de negocio del Departamento de TI y brinda como resultado el nivel para cada uno de los riesgos como se muestra a continuación (ver Apéndice N. Minutas de Reuniones con la Organización. – Tabla N24).

***Tabla 51**. Matriz de Riesgos*

ID	Riesgos	Probabilidad	Impacto	Calificación del riesgo	Nivel de riesgo
R-01	Materialización de riesgos debido a la ausencia de un proceso de gestión de riesgo que permita identificar y mitigar dichos riesgos.	5	5	5:5	**Alto**
R-02	Vulnerabilidades generadas por la falta de conocimiento y concienciación en colaboradores sobre la seguridad de información.	4	3	4:3	**Alto**
R-03	Errores en la ejecución y aumento de costos debido a la falta de políticas en la gestión de cambios con proveedores.	3	3	3:3	**Medio**
R-05	Pérdida o robo de información sensible de la organización o clientes por falta de controles en la gestión de medios extraíbles.	2	4	2:4	**Medio**
R-06	Presencia de software malicioso en los equipos de los colaboradores ante la ausencia de herramientas para la protección de los equipos personales.	4	2	4:2	**Medio**
R-07	Robo de equipos debido al traslado de los colaboradores y el teletrabajo.	3	2	3:2	**Medio**
R-08	Retrasos en operaciones y procesos por problemas que generan falta de disponibilidad de la información.	3	2	3:2	**Medio**
R-10	Instalación de malware por parte de colaboradores en los equipos debido a la falta de controles.	3	2	3:2	**Medio**
R-11	Retrasos y problemas en la cadena de suministro de	2	2	2:2	**Bajo**

ID	Riesgos	Probabilidad	Impacto	Calificación del riesgo	Nivel de riesgo
	tecnología debido a la falta de políticas.				

5.3.3.5. Respuestas ante los riesgos. En la siguiente **Tabla 52** se detallan los riesgos identificados con la respectiva estrategia de respuesta a ser aplicada. Las respuestas y estrategias fueron definidas para cada riesgo en reunión con los colaboradores del Departamento de TI (ver Apéndice N. Minutas de Reuniones con la Organización. – Tabla N24).

Tabla 52. *Respuesta Ante Riesgos.*

ID	Riesgos	Respuesta
R-01	Materialización de riesgos debido a la ausencia de un proceso de gestión de riesgo que permita identificar y mitigar dichos riesgos. **- Mitigar**	La organización destinará los recursos necesarios para definir e implementar el proceso de gestión de riesgos que ya se encuentra en planificación.
R-02	Vulnerabilidades generadas por la falta de conocimiento y concienciación en colaboradores sobre la seguridad de información. **- Mitigar**	La organización pronostica una mayor capacitación y entrenamiento de sus colaboradores como objetivo para el próximo año.
R-03	Errores en la ejecución y aumento de costos debido a la falta de políticas en la gestión de cambios con proveedores. **- Mitigar**	La organización realizará la gestión de cambios en servicios con proveedores a través del help desk.
R-04	Pérdida o robo de información sensible de la organización o clientes por falta de controles en la gestión de medios extraíbles. **- Mitigar**	Encriptar y proteger por medio de contraseñas la información contenida en medios extraíbles. Evitar la transferencia de información crítica o sensible a través de medios extraíbles.
R-06	Presencia de software malicioso en los equipos de los colaboradores ante la ausencia de herramientas para la protección de los equipos personales. **- Mitigar**	Prohibir el almacenamiento de información crítica o sensible en equipos personales y definir una política *Bring Your Own Device* (*BYOD*).

ID	Riesgos	Respuesta
R-07	Robo de equipos debido al traslado de los colaboradores y el teletrabajo. **- Mitigar**	Encriptar discos de almacenamiento en los equipos antes de ser entregados al responsable y aplicar el debido proceso de gestión de equipos perdidos o robados en caso de materializarse el riesgo.
R-08	Retrasos en operaciones y procesos por problemas que generan falta de disponibilidad de la información. **- Mitigar**	De acuerdo con la clasificación de información se pueden determinar los datos que requieren redundancia en su disponibilidad.
R-09	Modificación o eliminación no autorizada de la información debido a la falta de revisión de los permisos de acceso. **- Mitigar**	Establecer los permisos de acceso según lo establecido en la matriz RACI y realizar las respectivas revisiones y actualizaciones.
R-10	Instalación de malware por parte de colaboradores en los equipos debido a la falta de controles. **- Mitigar**	Encriptar puertos de activos con Licencia ESET antes de entregar a los responsables e implementar los programas de concientización requeridos.
R-11	Retrasos y problemas en la cadena de suministro de tecnología debido a la falta de políticas. **-Transferir**	Establecer políticas que apliquen a los contratos y verificar el cumplimiento por parte de proveedores.

5.3.4. Estudio financiero.

En el siguiente estudio se pretende determinar la estimación de los costos operativos y recursos necesarios para llevar a cabo el proyecto.

5.3.4.1. Objetivos Del Estudio. A continuación se presentan los objetivos propuestos para este estudio financiero.

5.3.4.1.1. Objetivo General. Determinar la factibilidad financiera correspondiente a la implementación de la propuesta de solución.

5.3.4.1.1. Objetivos Específicos. Se plantean los siguientes objetivos específicos para el presente estudio financiero.

- Analizar la necesidad y beneficios de la organización en la implementación del proyecto.
- Seleccionar el escenario con mayor beneficio para la implementación del proyecto.
- Estimar los recursos económicos necesarios para la implementación del proyecto.

5.3.4.2. Aspectos Por Considerar. El estudio financiero del proyecto tiene como principal función evidenciar de manera económica aquellos aspectos u observaciones mencionadas en los puntos anteriores de este documento.

El presente proyecto, al encontrarse enfocado en la mejora de la seguridad de la información dentro del Departamento de TI, tiene como objetivo conseguir diferentes beneficios intangibles que aseguren factores críticos en la protección de sus activos de información, aumento en la reputación de la organización y satisfacción de sus clientes, así como la estandarización adecuada del proceso de seguridad de la información que brinde mayor agilidad para su control y monitoreo.

Para identificar los principales atributos estratégicos relevantes para la organización se toman en cuenta las observaciones brindadas por los colaboradores especificadas en la sección 1.3. Planteamiento del Problema en el capítulo I de este documento así como los objetivos e indicadores clave de rendimiento del Departamento de TI presentados en la **Tabla 2** anteriormente.

Por esta razón el estudio financiero que se detalla a continuación estará basado en un análisis de costo beneficio que permita al Departamento de TI para conocer los costos de implementación necesarios que permitan obtener los beneficios estratégicos esperados a través de la certificación

Para alcanzar la certificación ISO 27001:2013 el Departamento de TI plantea su estrategia en dos etapas.

La primera de ellas consiste en ejecutar las diferentes actividades requeridas para atender las brechas identificadas, lo cual se pronostica realizar en un periodo de **seis meses**, según las estimaciones de tiempo por cada actividad brindados por los encargados del Departamento de TI (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N23).

Los costos identificados y estimados para esta primera etapa son los siguientes:

- **Costos iniciales:** costos asociados a la formulación del proyecto y evaluación de su viabilidad.
- **Costos de implementación:** costos estimados para ejecutar las actividades requeridas para cerrar las principales brechas.
- **Costos de mantenimiento:** costos estimados requeridos para la monitorización del SGSI y las auditorías internas.
- **Costos de adquisición:** costos evaluados en caso de ser necesaria la adquisición de licencias y/o servicios.
- **Costos de formación:** costos estimados para las capacitaciones de colaboradores y formación de auditor interno.

Para las estimar los costos de esta etapa se toma como referencia el promedio de costo por hora laboral que establece el Departamento de TI, el cual es de $23 por hora laboral, al mismo se le suma el 35% de las cargas sociales, lo que resulta en un total de $31.

En la segunda etapa necesaria para obtener la certificación contempla los costos asociados al proceso de consultoría y auditoría brindados por la empresa a cargo de emitir la certificación en ISO 27001:2013.

A pesar que esta segunda etapa se encuentra **fuera del alcance** en esta propuesta de solución, se toma como horizonte de evaluación financiera para determinar los posibles costos que representaría el desarrollo de la etapa para el Departamento de TI.

La primera certificación otorgada tiene un plazo de validez por tres años, debido a esto se evalúan los costos de certificación estimados para dicho periodo.

A continuación se detallan los costos estimados para ambas etapas.

5.3.4.2.1. Costos Iniciales. Los siguientes costos especificados en la **Tabla 53** corresponden a los recursos humanos, el tiempo y costo requeridos por la organización para llevar a cabo las tareas de formulación y evaluación de la viabilidad del proyecto.

Tabla 53. *Estimación de Costos Iniciales*

Actividad	Tiempo estimado	Recursos	Costo estimado
Anteproyecto y planificación.	40h	Practicante	$1240
Definir matriz de evaluación de seguridad de la información	150h	Practicante	$4.774
	15h	Director de seguridad	$1.178
Identificación de brechas y capacidad.	90h	Practicante	$2.790
	6h	Director de seguridad	$186

5.3.4.2.2. Costos de implementación. Estos costos corresponden a los esfuerzos necesarios de realizar por el departamento para solventar las brechas encontradas y generar

los procesos con la implementación de los controles y políticas que permitan establecer un SGSI más completo el cual permita la certificación deseada.

La organización cuenta con algunos recursos humanos para realizar estas tareas, sin embargo es necesario que se evalúe la posibilidad de realizar la contratación de un encargado de llevar a cabo la definición e implementación del proceso de gestión de riesgos de forma que no existan problemas en el desarrollo debido a limitaciones en el personal con el que cuenta actualmente el Departamento de TI.

Para efectos de la estimación se denomina el rol que desempeñará la persona encargada como “Ingeniero de Procesos”

La siguiente **Tabla 54** muestra los costos totales de implementación.

Tabla 54. *Estimación de Costos de Implementación.*

Actividad	Tiempo estimado	Recursos	Costo estimado
Establecer e implementar el proceso de gestión de riesgos	154h	Ingeniero de procesos	$4.774
	38h	Director de seguridad	$1.178
Definir las políticas y mejoras necesarias en el proceso de gestión de proveedores.	30h	Director de seguridad	$930
Definir los controles y políticas necesarias para la gestión de activos.	26h	Director de seguridad	$806
	26h	Soporte técnico	$806
Definir los criterios para la encriptación	5h	Director de seguridad	$155
Definir políticas para la redundancia de la disponibilidad de la información	5h	Director de seguridad	$155

5.3.4.2.3. Costos de mantenimiento. Los siguiente **Tabla 55** detalla los costos correspondientes al mantenimiento que requiere el SGSI para su respectiva monitorización y auditoría interna.

La estimación presentada a continuación corresponde a los costos mensuales de mantenimiento.

Tabla 55. *Estimación de Costos de Mantenimiento.*

Actividad	Tiempo estimado	Recursos	Costo estimado
Monitorización	8h	Director de seguridad	$248
Auditoría interna	4h	Auditor interno	$124

5.3.4.2.4. Costos de adquisición. Para implementar los controles necesarios la organización debe realizar estudios que le permitan determinar si requiere de un servidor que brinde las características necesarias para garantizar la seguridad y redundancia de la información crítica.

Además, se debe evaluar la necesidad de adquirir una licencia de antivirus, a pesar que actualmente se cuenta con la licencia de *ESET Endpoint Protection Standard antivirus* se debe analizar si la empresa requiere adquirir la licencia *ESET Protect Complete* que brinde la seguridad necesaria en todos los dispositivos.

Para esto se realizan las siguientes estimaciones del costo de los activos, dicha estimación se realiza a partir de cotizaciones realizadas por la organización en servicios de infraestructura para un servidor con características específicas para la organización que son reservadas para resguardar la confidencialidad, así como los datos obtenidos de ESET (2021) para estimar los costos de la licencia mencionada. En la siguiente **Tabla 56** se muestran los

costos de adquisición que debe ser tomado en cuenta en caso de requerir los activos por parte de la organización.

La estimación presentada a continuación corresponde a los costos mensuales de los servicios adquiridos. .

Tabla 56. *Estimación de Costos de Adquisición*

Activo	Estimación de costo
Servidor	$3.900
Licencia ESET Protect Complete	$360

La organización pretende optar por la opción de infraestructura como servicio (IaaS, por sus siglas en inglés), de la misma forma, la licencia de antivirus es brindada a través de servicios en la nube, por esta razón el costo estimado corresponde al pago mensual que debería asumir la organización en caso de contratar los servicios.

El centro de datos en el que se encuentra el servidor cuenta con certificaciones en ISO 27001 y Tier III, por lo que brinda la seguridad apropiada para la organización.

5.3.4.2.5. Costos de Formación. En la siguiente **Tabla 57** se muestran los costos de formación correspondientes al desarrollo de un auditor interno que será el encargado realizar las verificaciones de cumplimiento y las actualizaciones necesarias al SGSI, así como las capacitaciones necesarias a los colaboradores del Departamento de TI que garanticen la adecuada implementación de los procedimientos establecidos por el sistema.

Para llevar a cabo las auditorías internas requeridas por el SGSI, el Departamento de TI planea capacitar al analista de negocio CRM con el que cuenta actualmente, de forma que sea el responsable encargado de realizar dicho proceso. La organización pronostica realizar las respectivas capacitaciones cada seis meses.

***Tabla 57**. Estimación de Costos de Formación*

Actividad	Tiempo estimado	Recursos	Costo estimado
Capacitaciones de auditor interno	4h	Director de seguridad	$124
	4h	Auditor interno	$124
Capacitaciones en el uso del SGSI	4h	Director de seguridad	$124
	4h	Soporte técnico (x2)	$248
	4h	Ingeniero de procesos	$124

5.3.4.2.6. Costos de certificación. Una vez la organización haya realizado las inversiones necesarias para atacar las brechas de seguridad identificadas se deben contemplar los costos relacionados con la certificación.

Para esto se realizó una solicitud de cotización en los tres proveedores, especificados en la **Tabla 32** del Estudio de Mercado en este documento, para obtener los datos del proceso que incluye los costos de auditoría y certificación. Sin embargo, solo fue recibida la respectiva cotización por parte del Instituto de Normas Técnicas de Costa Rica (INTECO), la cual se detalla en la siguiente **Tabla 58** que muestra el desglose de los costos para los tres primeros años que tiene vigencia la certificación.

***Tabla 58.** Cotización INTECO*

Producto	Duración/ Cantidad	Impuestos	Precio por día / unidad	Precio total
Año 1				

Producto	Duración/ Cantidad	Impuestos	Precio por día / unidad	Precio total
Análisis documental	5 días	Tarifa General 13%	$1,100.00	$6,215.00
Evaluación de cumplimiento	6 días	Tarifa General 13%	$1,100.00	$7,458.00
Emisión, mantenimiento o anualidad de certificación	1 unidad	Tarifa General 13%	$450.00	$508.50
			Subtotal	**$14,181.50**
Año 2				
Auditoría de seguimiento 1	4 días	Tarifa General 13%	$1,100.00	$4,972.00
Emisión, mantenimiento o anualidad de certificación	1 unidad	Tarifa General 13%	$450.00	$508.50
			Subtotal	**$5,480.50**
Año 3				
Auditoría de seguimiento 1	4 días	Tarifa General 13%	$1,100.00	$4,972.00
Emisión, mantenimiento o anualidad de certificación	1 unidad	Tarifa General 13%	$450.00	$508.50
			Subtotal	**$5,480.50**

Producto	Duración/ Cantidad	Impuestos	Precio por día / unidad	Precio total
			Subtotal	**$22,250.00**
			Impuestos	$2,892.50
			Total	**$25,142.50**

Fuente: Cotización enviada por INTECO (Ver Apéndice K. Cotización INTECO.).

5.3.4.3. Beneficios Financieros y no Financieros. Para esta sección se presentan los beneficios esperados al implementar la propuesta planteada desde una perspectiva tanto económica como estratégica.

5.3.4.3.1. Beneficios Financieros. Debido a la ausencia de datos cuantitativos que permitan determinar los beneficios financieros percibidos por la organización al implementar la propuesta, se establecen supuestos que permitan realizar las debidas estimaciones basadas en posibles escenarios presentados a partir de la materialización del riesgo más crítico para la organización.

Actualmente la organización presenta la ausencia de un proceso definido para la gestión de riesgos, esto provoca una alta probabilidad de impacto al momento de materializarse un riesgo crítico.

A continuación se presentan dos posibles escenarios con supuestos asociados al impacto económico que se estima en caso de materializarse el riesgo que corresponde con la generación de vulnerabilidades debido a la falta de conocimiento por parte de los colaboradores en la seguridad de la información, ya que, a través de phishing o ransomware, se pueden generar incidentes que provoquen el secuestro o daño de información crítica o se

bloquee el acceso a los usuarios del sistema más crítico para la organización, Microsoft DevOps Server.

Los escenarios presentados a continuación son establecidos en conjunto con el Director de Seguridad, Analista de Negocio de TI y Analista de Negocio CRM (ver Apéndice N. Minutas de Reuniones con la Organización. – Apartado: Tabla N25).

- **Escenario Catastrófico:** para este escenario se realiza un análisis de las afectaciones percibidas en caso de sufrir un incidente en la disponibilidad e integridad de la información contenida en Microsoft DevOps Server, el cual corresponde con el sistema más crítico de la organización.

  En este caso se supone una disponibilidad nula del sistema y la información para todos los usuarios, estimándose el impacto económico en la productividad que representaría el incidente, como se muestra en la siguiente **Tabla 59**. Escenario Catastrófico..

***Tabla 59**. Escenario Catastrófico.*

Escenario catastrófico				
Incidente	**Cantidad de usuarios afectados**	**Porcentaje de impacto en la productividad por hora**	**Costo del impacto por hora**	**Estimación de impacto económico por hora**
Caída, secuestro o daño de información en Azure DevOps Server.	150	-50%	$2,325	$348,750

- **Escenario Negativo:** para este segundo escenario se supone que, en caso de sufrir un incidente en la disponibilidad e integridad de la información contenida en el sistema

más crítico, se ve afectado un único usuario. Esto puede ser causado debido a bloqueos en el acceso o robo de contraseña, estimándose el impacto económico en la productividad que representaría el incidente, como se muestra en la siguiente **Tabla 60**. Escenario Negativo..

***Tabla 60**. Escenario Negativo.*

Escenario Negativo				
Incidente	**Cantidad de usuarios afectados**	**Porcentaje de impacto en la productividad por hora**	**Costo del impacto por hora**	**Estimación de impacto económico por hora**
Pérdida temporal del acceso al sistema Azure DevOps Server.	1	-50%	$15.5	$15.5

Al llevar a cabo la propuesta planteada la organización podrá tomar las medidas adecuadas para mitigar el riesgo desde diferentes estrategias como se menciona a continuación.

- **Respaldos:** mantener los respaldos de información crítica permite tener la disponibilidad para mantener las operaciones de usuarios afectados, al menos de forma local, reduciendo el impacto generado.
- **Encriptación de datos:** realizar la encriptación de datos sensibles reduce la posibilidad de lectura y escritura ante un incidente por secuestro o robo de información.
- **Redundancia:** contar con la redundancia necesaria para mantener la disponibilidad de sistemas críticos permite mitigar los riesgos asociados por la caída de sistemas, servicios o bloqueos en el acceso provocados *malware* o *phishing.*

5.3.4.3.2. Beneficios No Financieros. Al tener como objetivo una futura certificación en la norma ISO 27001:2013 se requiere tomar en cuenta los beneficios esperados por la organización desde una perspectiva estratégica. Por esta razón se muestran los siguientes beneficios no financieros esperados al implementar la propuesta.

- Reducción de los riesgos relacionados con la seguridad de la información a través de la implementación del SGSI con sus respectivas políticas y controles.
- Reducción de costos al prevenir de manera más efectiva posibles incidentes de seguridad de la información.
- Estandarización del proceso de la gestión de seguridad de la información.
- Organización efectiva en el control y gestión de los procesos.
- Reducción en los tiempos de operación.
- Mayor control sobre la información sensible de la organización.
- Mayor concientización en los colaboradores sobre la seguridad de la información.
- Identificación oportuna y corrección de vulnerabilidades.
- Proteger y mejorar la reputación de la empresa.
- Ventaja competitiva al brindar mayor confianza y satisfacción para sus clientes.
- Cumplimiento de la legislación y regulaciones pertinentes.

5.3.4.3.3. Análisis de Costo vs Beneficio. En esta sección se muestran los costos totales que la organización debe asumir en los primeros seis meses de implementación de la propuesta, para esto se detallan los costos de cada una de las etapas, mencionadas anteriormente, en función del plazo que requiere cada una de las etapas para su ejecución.

En cuanto a los costos de certificación, INTECO detalla en su cotización los diferentes costos que la organización debe cancelar correspondientes a los tres años de vigencia de la

primera certificación, para esto se realiza la respectiva estimación de acuerdo con los datos presentados en la **Tabla 58.** Cotización INTECO

Para estimar los beneficios percibidos por la organización se toman en cuenta los gastos que la empresa debe asumir en caso de materializarse el escenario catastrófico detallado anteriormente en la **Tabla 59**, los cuales podrían ser mitigados con la implementación de la propuesta.

Es importante recalcar que los costos iniciales del proyecto no deben ser tomados en cuenta en el análisis de costo-beneficio debido a que la organización ya asumió dichos costos a lo largo del tiempo en que fue desarrollado este proyecto.

En la siguiente **Tabla 61** se desglosa el análisis de los costos y beneficios estimados para el proyecto.

Tabla 61. *Desglose de Costos y Beneficios Estimados*

Detalle	Costo Total
Costos de implementación	$2,857
Costos de mantenimiento	$2,232
Costos de adquisición	$25.560
Costos de formación	$744
Costos de certificación	$25,142
Total de costos	**$56,535**
Ahorro de gastos estimado	**$348,750**
Beneficios Netos	**$292,215**

5.3.4.3.4. Valor Presente y Valor Futuro. Para determinar el valor del dinero en el tiempo se toma el total de costos, los beneficios netos y la inflación del dólar para realizar los siguientes cálculos.

A continuación se muestran los montos percibidos en el presente.

- **Total de costos presentes:** $56,535
- **Beneficios netos presentes:** $292,215

Para calcular el valor futuro de los costos y beneficios se toman los siguientes datos para aplicar la fórmula de interés compuesto.

$$Valor\ Futuro\ =\ VF$$

$$Valor\ Presente\ =\ VP$$

$$Inflación\ del\ dólar\ =\ i$$

$$VF = VP * (1 + i)^n$$

Tomando como referencia los datos de OECD (2021), el cual pronostica una inflación del dólar de 2,5% para el año 2022, se proceden a realizar los siguientes cálculos.

- **Total de costos futuros:** A continuación se realizan los cálculos para determinar el valor futuro de los costos totales.

$$VF = VP * (1 + i)^n$$

$$VF =\ 56{,}535 * (1 + 0{,}025)^3$$

$$VF =\ 60{,}882$$

Al aplicar la formula anterior se logra estimar el total de costos con un valor futuro de: $60,882.

- **Beneficios netos futuros:** A continuación se realizan los cálculos para determinar el valor futuro de los beneficios netos.

$$VF = VP * (1 + i)^n$$

$$VF = 292{,}215 * (1 + 0{,}025)^3$$

$$VF = 314{,}683$$

Al aplicar la formula anterior se logra estimar el total de beneficios netos con un valor futuro de: $314,683.

5.3.4.3.5. Relación Beneficio Costo. La relación Beneficio Costo permite determinar la viabilidad basado en los beneficios esperados y los costos totales asociados del proyecto.

Para determinar esta relación se compara el resultado con 1, de la siguiente manera.

$\frac{Beneficios}{Costos} > 1$, refleja que los beneficios son mayores a los costos del proyecto, demostrando la viabilidad del mismo.

$\frac{Beneficios}{Costos} = 1$, refleja que los beneficios son iguales a los costos del proyecto, donde no es posible determinar un beneficio o ganancia.

$\frac{Beneficios}{Costos} < 1$, refleja que los beneficios son menores a los costos del proyecto, indicando que no existe viabilidad.

Una vez se estima el valor futuro de los montos asociados a la inversión para el periodo de tres años que corresponde al plazo de validez de la certificación, se realiza el siguiente cálculo para determinar la relación beneficio-costo del proyecto.

$$\frac{Beneficios\ netos\ futuros}{Total\ de\ costos\ futuros}$$

$$\frac{314{,}683}{60{,}882} = 5{,}16$$

$$5{,}16 > 1$$

A partir del cálculo anterior se logra determinar la viabilidad del presente proyecto al identificar un mayor beneficio percibido en relación con los costos asociados.

5.3.4.4. Conclusiones del Estudio Financiero. A continuación se presentan las conclusiones del estudio financiero realizado.

- Los esfuerzos e inversiones de la organización para llevar a cabo la propuesta se enfocan en recursos humanos y horas humanas para definir e implementar los procesos y políticas requeridas para atender las brechas en seguridad de la información encontradas.
- Se requiere de estudios específicos para determinar los costos de adquisición necesarios para contar con los activos indispensables para la implementación.
- A pesar de que los mayores beneficios esperados son de carácter estratégico se pueden establecer estimaciones basadas en riesgos y escenarios que demuestren los montos económicos que la organización se puede ahorrar con la implementación de la propuesta.
- Para garantizar una adecuada implementación de la propuesta se requiere una reestructuración del Departamento de TI que permita la capacitación y contratación de personal calificado para llevar a cabo las tareas necesarias.
- Se logra determinar la viabilidad del proyecto a partir del análisis de la relación entre el costo y el beneficio estimados.

5.3.5. Plan de Implementación

Para establecer un plan que permita la implementación de la propuesta se requieren establecer los recursos humanos y financieros que serán necesarios para llevar a cabo las diferentes actividades.

5.3.5.1. Objetivos del plan. A continuación se muestran los objetivos definidos para el plan de implementación.

5.3.5.1.1. Objetivo general. Ofrecer una guía a Mobilize.Net para la implementación de las acciones necesarias para el cierre de brechas identificadas en materia de gestión de seguridad de la información en el Departamento de TI.

5.3.5.1.2. Objetivos Específicos. A continuación se presentan los objetivos específicos definidos para el plan.

- Identificar los roles y responsabilidades necesarias para llevar a cabo las actividades definidas en el caso de negocio.
- Programar la dotación de recursos financieros y humanos a lo largo de las fases del proyecto.

5.3.5.2. Descripción. El siguiente plan contempla la implementación de la primera fase del proyecto que establece las actividades necesarias para atacar las principales brechas identificadas en el Departamento de TI.

La segunda fase que no ha sido tomada en cuenta para esta propuesta, requiere de un proceso similar aplicado a los departamentos de la organización que correspondan, de manera que se defina la implementación de las tareas identificadas, por medio de la consultoría con la organización certificadora, que deban ejecutarse para preparar a la empresa de cara a la certificación en la norma ISO 27001:2013.

Para llevar a cabo esta propuesta de implementación se deben tomar en cuenta los siguientes aspectos que permitan la aplicación del modelo RACI para desarrollar la matriz.

- Identificar los actores del proceso de gestión de seguridad de la información.
- Definir las actividades del proceso.
- Definir los roles y responsabilidades de los actores para cada actividad.

Seguidamente se procede a definir el proceso que permita crear la matriz RACI.

5.3.5.2.1. Proceso de Matriz RACI. El proceso detallado a continuación permitirá establecer la matriz RACI a través de la ejecución de cada una de las etapas mencionadas anteriormente.

***5.3.5.2.2. Identificar los actores del proceso de gestión de seguridad de la información*.** Para esta etapa se requiere definir los diferentes roles que asumirán los involucrados en el proceso.

- **Responsable:** es la persona encargada de ejecutar la tarea, por lo general debe existir un único responsable a cargo de cada tarea.
- **Aprobador:** encargado de designar a la persona responsable de la tarea y controlar su correcta ejecución para la rendición de cuentas. En algunos casos el responsable y el aprobador podrían ser la misma persona.
- **Consultado:** involucrado con información o capacidad relevante que puede ser consultada para la ejecución adecuada de la tarea.
- **Informado:** involucrado que debe ser informado de los avances y resultados obtenidos a lo largo de la ejecución por parte del responsable. La comunicación hacia este rol se realiza de manera unidireccional.

5.3.5.2.3. Identificación de Actores. En la siguiente **Tabla 62** se muestran los actores identificados en el Departamento de TI que tendrán roles específicos en las diferentes actividades.

***Tabla 62**. Actores en el Proceso de Implementación.*

ID	Actor
A-01	Director de seguridad
A-02	Analista de negocio
A-04	Ingeniero de procesos
A-05	Soporte técnico
A-06	Auditor interno

5.3.5.2.4. Principales Actividades del Proceso. Para implementar la propuesta planteada se requieren llevar a cabo las siguientes actividades detalladas en la **Tabla 63**.

***Tabla 63**. Actividades a Implementar.*

ID	Actividad
Act-01	Establecer e implementar el proceso de gestión de riesgos
Act-02	Definir las políticas y mejoras necesarias en el proceso de gestión de proveedores.
Act-03	Definir los controles y políticas necesarias para la gestión de activos.
Act-04	Definir los criterios para la encriptación
Act-05	Definir políticas para la redundancia de la disponibilidad de la información
Act-06	Capacitaciones a los colaboradores en el uso del SGSI
Act-07	Capacitaciones de auditor interno
Act-08	Monitorización del SGSI
Act-09	Auditoria interna

Las actividades mencionadas anteriormente permitirán la implementación de las acciones a tomar para atender las brechas identificadas, capacitar a los usuarios y auditor interno y monitorización para la mejora continua del sistema de gestión de seguridad de la información.

5.3.5.2.5. Matriz RACI. Una vez se identifican los aspectos necesarios para la implementación de la propuesta se procede a definir la siguiente matriz RACI presentada en la **Tabla 64** la cual establece los roles que tomará cada uno de los actores para las diferentes actividades a ejecutar.

Tabla 64. *Matriz RACI.*

Actividad / Actor	Director de Seguridad	Analista de Negocios	Ingeniero de Procesos	Soporte Técnico	Auditor de Procesos
Establecer e implementar el proceso de gestión de riesgos	*Aprobador*	*Consultado*	***Responsable***	*Informado*	-
Definir las políticas y mejoras necesarias en el proceso de gestión de proveedores.	***Responsable*** */ Aprobador*	*Consultado*	-	*Informado*	-
Definir los controles y políticas necesarias para la gestión de activos.	*Aprobador*	*Consultado*	-	***Responsable***	-
Definir los criterios para la encriptación	***Responsable*** */ Aprobador*	*Consultado*	-	*Informado*	-

Actividad / Actor	Director de Seguridad	Analista de Negocios	Ingeniero de Procesos	Soporte Técnico	Auditor de Procesos
Definir políticas para la redundancia de la disponibilidad de la información	***Responsable*** */ Aprobador*	*Consultado*	-	*Informado*	-
Capacitaciones a los colaboradores en el uso del SGSI	***Responsable*** */ Aprobador*	*Consultado*	*Informado*	*Informado*	-
Capacitaciones de auditor interno	***Responsable*** */ Aprobador*	*Consultado*	-	-	*Informado*
Monitorización del SGSI	***Responsable*** */ Aprobador*	*Consultado*	-	-	*Informado*
Auditoría interna	*Aprobador*	*Consultado*	-	-	***Responsable***

5.3.5.2.6. Cronograma. A continuación se presenta el cronograma propuesto para la implementación de las actividades con sus respectivas estimaciones en recursos financieros y tiempos de ejecución necesarios, según los datos mostrados en el presente Caso de Negocio.

El desarrollo del cronograma fue realizado a través de la aplicación *Instagantt* (2021) y se muestra en la siguiente **Figura 13**. Cronograma de Implementación.

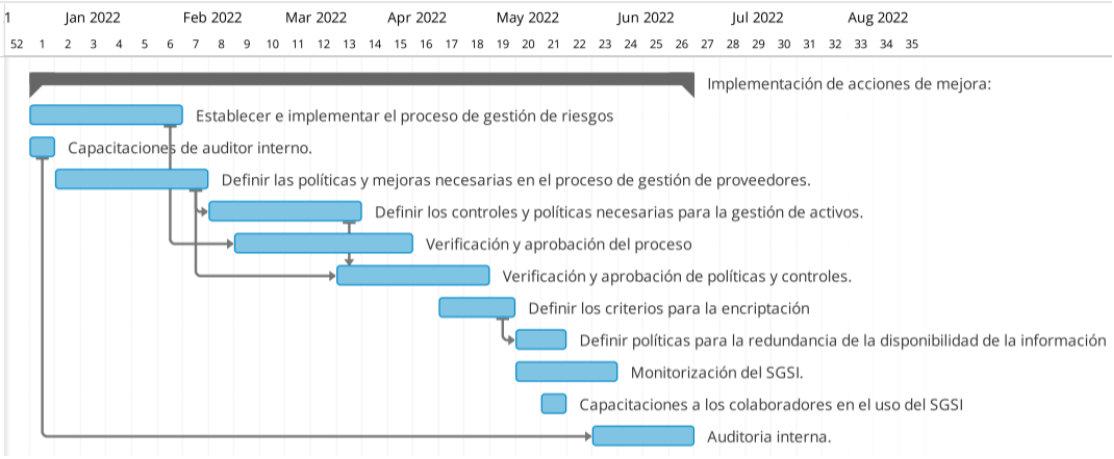
***Figura 13**. Cronograma de Implementación.*

Cronograma de Implementación

Read-only view, generated on 05 Nov 2021

Instagantt

	ACTIVITIES	ASSIGNEE	EH	EC	START	DUE
	Implementación de acciones de mejora:		380h	$11.780,00	03/Jan	01/Jul
1	Establecer e implementar el proceso de gestión de ries...	Ingeniero de Pr...	154h	$4.774,00	03/Jan	11/Feb
2	Capacitaciones de auditor interno.	AI, Dd	8h	$248,00	03/Jan	07/Jan
3	Definir las políticas y mejoras necesarias en el proceso ...	Director de Seg...	30h	$930,00	10/Jan	18/Feb
4	Definir los controles y políticas necesarias para la gestió...	Soporte Técnico	26h	$806,00	21/Feb	28/Mar
5	Verificación y aprobación del proceso	Director de Seg...	38h	$1.178,00	03/Mar	14/Apr
6	Verificación y aprobación de políticas y controles.	Director de Seg...	26h	$806,00	28/Mar	02/May
7	Definir los criterios para la encriptación	Director de Seg...	5h	$155,00	29/Apr	13/May
8	Definir políticas para la redundancia de la disponibilidad...	Director de Seg...	5h	$155,00	16/May	27/May
9	Monitorización del SGSI.	Director de Seg...	48h	$1.488,00	16/May	10/Jun
10	Capacitaciones a los colaboradores en el uso del SGSI	Dd, ST, Id	16h	$496,00	23/May	27/May
11	Auditoria interna.	Auditor Interno	24h	$744,00	06/Jun	01/Jul



En la siguiente **Figura 14** se muestra con mayor detalle el resumen de los recursos humanos y financieros necesarios para la implementación de las tareas presentadas en el cronograma.

Figura 14. *Recursos Necesarios Para la Implementación de la Propuesta.*

Considerar los recursos presentados permitirá al Departamento de TI poder ejecutar adecuadamente las actividades necesarias para la implementación de la propuesta presentada.

5.3.5.2.7. Hojas de verificación. Como parte de la evaluación requerida para el caso de negocio se propone que la organización utilice como herramienta la matriz de Evaluación de Seguridad de la Información presentada en el Apéndice H. Matriz de Evaluación de la Seguridad de la Información.

Capítulo VI: Conclusiones

A continuación se presentan las conclusiones del proyecto para cada uno de los objetivos específicos definidos.

Objetivo I: Analizar la situación actual de la empresa en relación con la identificación de controles en seguridad de la información necesarios y el cumplimiento de los requerimientos recibidos.

I. Se identifica que el Departamento de TI cuenta con los recursos organizativos, técnicos y estratégicos para cumplir con los requerimientos de los clientes y la organización en materia de seguridad de la información a través de políticas y controles establecidos y documentados.

Objetivo II: Establecer los aspectos estratégicos, técnicos y de gestión necesarios para el desarrollo de la propuesta.

II. De acuerdo a los controles establecidos en la norma ISO 27001:2013 se identifica que el 55% de las áreas de control en el Departamento de TI, cuentan con un nivel de capacidad mayor al 85% en el cumplimiento de sus controles.

III. Se identifican las brechas en seguridad de la información de las áreas con un nivel de capacidad menor al 85% como primer paso para definir las acciones a tomar por parte del Departamento de TI con miras a la certificación. Las brechas identificadas corresponden a las siguientes áreas de control.

a. Gestión de riesgos.
b. Relación con proveedores.
c. Administración de activos.
d. Organización de la seguridad de la información.
e. Criptografía.
f. Tercerización.

g. Servicios en la nube.

h. Seguridad de la información en la gestión de la continuidad del negocio.

Objetivo III: Desarrollar los estudios de factibilidad necesarios que permitan determinar la viabilidad de la certificación.

IV. El Departamento de TI carece de un proceso para la gestión de riesgos, el cual es indispensable para obtener la certificación, siendo esta la principal brecha a cerrar.

V. Se requiere generar acciones de mejora que permitan cerrar las brechas identificadas y alinear el sistema de gestión de la seguridad de la información del Departamento de TI con los requerimientos establecidos por la norma ISO 27001:2013.

Objetivo IV: Elaborar una propuesta de implementación que brinde la guía necesaria para obtener la certificación en ISO 27001:2013 para el departamento de TI en la empresa.

VI. La implementación del SGSI a través de la infraestructura de TI que soporte adecuadamente los controles y procedimientos definidos con la respectiva monitorización del cumplimiento por parte de un responsable, permite al departamento de TI alcanzar sus objetivos estratégicos e indicadores clave de rendimiento establecidos por la alta dirección.

VII. A partir del desarrollo del estudio de mercado, estudio técnico, análisis de riesgos y estudio financiero se logra ratificar la viabilidad de un sistema de gestión de seguridad de la información que permita preparar al Departamento de TI para la valoración externa con miras a la certificación.

VIII. A partir de la identificación de las actividades necesarias, los recursos necesarios y el plazo de tiempo establecido por el Departamento de TI se podrá llevar a cabo la adecuada implementación de las acciones de mejora planteadas para su SGSI.

Capítulo VII: Recomendaciones

A continuación se presentan las recomendaciones brindadas de acuerdo a las conclusiones obtenidas del proyecto.

I. Se recomienda evaluar periódicamente la capacidad de la infraestructura de TI y los recursos disponibles de forma que se destinen las inversiones necesarias para la implementación de las políticas, procedimientos y controles necesarios por parte del Departamento de TI para la gestión de seguridad de la información que le permita el adecuado cumplimiento de los requerimientos de sus clientes.

II. Mantener la mejora continua en las áreas de control que cuentan con un nivel de capacidad mayor al 85% de forma que sea posible llevarlas, progresivamente, a un cumplimiento del 100%.

III. Se recomienda concentrar los esfuerzos en atacar las brechas de acuerdo a la priorización establecida, de manera que se atiendan los aspectos más críticos lo antes posible.

IV. Definir e implementar el proceso de gestión de riesgos que responda a la realidad de la organización y permita cumplir con los requerimientos, tanto de la norma ISO 27001:2013 como de los clientes de la organización.

V. Utilizar el presente caso de negocio con la propuesta de solución a las brechas identificadas como guía para establecer las acciones que se requieren llevar a cabo para la implementación de los procedimientos, políticas y controles necesarios que permitan en alineamiento del SGSI con la norma ISO 27001:2013.

VI. Mantener el cumplimiento de los indicadores clave de rendimiento a través de la verificación permanente de los controles implementados a través de la infraestructura de TI por parte de los encargados en el Departamento de TI.

VII. Alinear adecuadamente el SGSI a la realidad de la organización y sus recursos disponibles de forma que se gestione adecuadamente la seguridad de la información que permita preparar a la organización hacia la certificación ISO 27001:2013.

VIII. Valorar los recursos necesarios para la implementación del presente caso de negocio dentro del presupuesto y la planificación del próximo periodo de acuerdo a la viabilidad demostrada desde la perspectiva técnica, estratégica y de gestión para la ejecución de las acciones de mejora en el plazo establecido.

Capítulo VIII: Referencias Bibliográficas

Alderete, M., & Gutiérrez, L. (2012). TIC y productividad en las industrias de servicios en Colombia. *Lecturas de economía*, *77*, 163–188.

Baca Urbina, G. (2016). *Evaluacion De Proyectos* (1.ª ed.). McGraw-Hill.

Barrio Juárez, F. A. (2020, 14 julio). *La crisis del Covid-19 ha impulsado los intentos de ciberataques a empresas • Red Forbes* •. Forbes México. Recuperado 13 de agosto de 2021, de https://www.forbes.com.mx/la-crisis-del-covid-19-ha-impulsado-los-intentos-de-ciberataques-a-empresas/

Blokdyk, G. (2017). *ISO Iec 27000: Upgrader's Guide*. Createspace Independent Publishing Platform.

COBIT 2019 Framework: Introduction and Methodology. (2018). Isaca.

Definition of Cybersecurity - Gartner Information Technology Glossary. (s. f.). Gartner. Recuperado 1 de septiembre de 2021, de https://www.gartner.com/en/information-technology/glossary/cybersecurity

Definition of IT Governance (ITG) - Gartner Information Technology Glossary. (s. f.). Gartner. Recuperado 1 de septiembre de 2021, de https://www.gartner.com/en/information-technology/glossary/it-governance

D. G. Rosado, L. E. Sánchez, D. Mellado, E. F. Medina. (2014). Seguridad en el grado de informática acorde a las certificaciones profesionales. Researchgate.net. https://www.researchgate.net/profile/Luis-Enrique-Sanchez-Crespo/publication/272486839_Contenido_de_Seguridad_en_el_Grado_de_Informatica_acorde_a_las_certificaciones_profesionales/links/54e5d54c0cf2cd2e028b34fa/Contenido-de-Seguridad-en-el-Grado-de-Informatica-acorde-a-las-certificaciones-profesionales.pdf

Diana Marcela Guerrero Juan Camilo Martinez Díaz. (2016). Propuesta de un sistema de gestión de la seguridad de la información para entidades dedicadas al servicio de Outsourcing de TI.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of information security, 04(02), 92–100.

ESET. (2020, diciembre). *TENDENCIAS EN CIBERSEGURIDAD PARA EL 2021: Mantenerse seguro en tiempos de incertidumbre*. https://www.welivesecurity.com/wp-content/uploads/2020/12/Cybersecurity_Trends_2021_ES.pdf

ESET. (2021, junio). *ESET Security Report Latinoamérica 2021*. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Garcia, D., Sánchez, L., Mellado, D., & Fernández, E. (2014, septiembre). *Contenido de Seguridad en el Grado de Informática acorde a las certificaciones profesionales*. researchgate.net. https://www.researchgate.net/publication/272486839_Contenido_de_Seguridad_en_el_Grado_de_Informatica_acorde_a_las_certificaciones_profesionales

Georges, A., & Thorp, J. (2007). *Enterprise Value: Governance of IT Investments, The Business Case*. IT Governance Institute.

Guerrero, D., & Martinez, J. (2016). *PROPUESTA DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA ENTIDADES DEDICADAS AL SERVICIO DE OUTSOURCING DE TI.* repository.udistrital.edu.co. https://repository.udistrital.edu.co/handle/11349/8320

Hernández, R., Mendoza, P., Méndez, S., & Cuevas, A. (2019). *Metodología de la Investigación para bachillerato* (2.ª ed.). McGraw-Hill.

Hernández Sampieri, R., Collado, C. F., & Lucio, P. B. (2014). *Metodología de La Investigación* (6.ª ed.). MC Graw Hill.

Hernández Sampieri, R., Torres, P. M., Valencia, S. M., & Romo, A. C. (2019). *Metodología de la Investigación para bachillerato* (2.ª ed.). McGraw-Hill.

Hernández-Sampieri, R., & Torres, M. C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (1.ª ed.). McGraw Hill Interamericana.

Holt, A., & Holt, A. L. (2013). *Governance of It: An Executive Guide to ISO/Iec 38500*. BCS, the Chartered Institute for IT.

Instagantt. (2021). Instagrantt. https://app.instagantt.com/r#projects/wb96TKkZP5BSW5lzztkW/wb96TKkZP5BSW5lzztkW

International Organization for Standardization. (2013a). *ISO/IEC 27001:2013, Second Edition: Information technology - Security techniques - Information security management systems - Requirements* (2.ª ed.). Multiple. Distributed through American National Standards Institute (ANSI).

International Organization for Standardization. (2013b). *ISO/IEC 27002:2013, Second Edition: Information technology Security techniques Code of practice for information security controls* (2.ª ed.). Multiple. Distributed through American National Standards Institute (ANSI).

International Organization for Standardization. (2016). *ISO/IEC 27000:2016, Fourth Edition: Information technology - Security techniques - Information security management systems - Overview and vocabulary* (4.ª ed.). Multiple. Distributed through American National Standards Institute (ANSI).

INTERPOL. (2020, agosto). *CIBERDELINCUENCIA: EFECTOS DE LA COVID-19*. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Iso/Tmb. (2009). *ISO/IEC 31010:2009, Risk management - Risk assessment techniques*. Multiple. Distributed through American National Standards Institute (ANSI).

ITIL foundation (4th ed.). (2019). Tso, the Stationery Office.

Linkedin. (2021). www.mobilize.net. https://cr.linkedin.com/company/mobilize-net

López, A. (2005). Glosario. Iso27000.es. https://www.iso27000.es/glosario.html

MobilizeNet. (2021, 8 mayo). YouTube. https://www.youtube.com/watch?v=DIhmB7S-0Vk&t=4s&ab_channel=Mobilize.net

Nuevas Tecnologías & Innovación. (2007, enero). *Comunicación Empresarial*, *15*. https://www.zucchetti.es/wp-content/uploads/press_release/EspecialLaGaceta180107.pdf

Prices - Inflation forecast - OECD Data. (2021). OECD. https://data.oecd.org/price/inflation-forecast.htm#indicator-chart

Protect Complete. (2021). ESET. https://www.eset.com/bo/empresas/complete-protection-bundle/

Quirós, L. V. (2013, 24 noviembre). *¿Cuánto cuesta certificarse con una norma ISO?* El Financiero. https://www.elfinancierocr.com/negocios/cuanto-cuesta-certificarse-con-una-norma-iso/Y4B47MXQHRGM7HH47FG3KZR2HQ/story/

Razo, M. C. (2011). *Como Elaborar Y Asesorar Una Investigacion De Tesis* (2.ª ed.). PRENTICE HALL/PEARSON.

Saavedra García, M. L., & Tapia Sánchez, B. (s/f). Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento. Redalyc.org. Recuperado el 3 de septiembre de 2021, de https://www.redalyc.org/pdf/823/82326270007.pdf

[UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS]. https://repository.udistrital.edu.co/bitstream/handle/11349/8320/GuerreroDiana%20Marcela%202016.pdf?sequence=1&isAllowed=y

Valencia, F., & Orozco, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000*. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=6672188

Capítulo IX: Anexos

Anexo 1 Carta de revisión Filológica

CARTA DE FILÓLOGA

Heredia, 05 de noviembre del 2021

Señores (as)

Área Académica de Administración de Tecnologías de Información

Tecnológico de Costa Rica

Estimados señores (as)

La suscrita Edith Raissa Pizarro Alfaro con cédula de identidad No. 401780133, profesional en Filología, hace constar que revisó el documento que lleva por título **Propuesta de viabilidad mediante un caso de negocio en el Departamento de Tecnologías de Información para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013 en la empresa Mobilize.NET ,** del estudiante **Bryan Daniel Blanco Morales,** al cual se le aplicaron las revisiones y observaciones relacionadas con aspectos de construcción gramatical, ortografía, redacción, entre otros.

Dado lo anterior, certifico que el documento contiene las observaciones y correcciones quedando de conformidad con lo pactado.

Atentamente

Firmado por EDITH RAISSA PIZARRO ALFARO (FIRMA)
PERSONA FISICA, CPF-04-0178-0133. Fecha declarada: 05/11/2021 07:28 PM
Esta representación visual no es una fuente de confianza, valide siempre la firma.

Licda. Edith Raissa Pizarro Alfaro

Código 35554

Anexo 2. Certificado de Participación en Webinar de Auditoría.

Capítulo X: Apéndices

Apéndice A. Entrevista con Analista de Negocio de TI.

Entrevista 1

Fecha: 26/06/2021

Objetivo de la entrevista: Determinar los problemas presentados por el Departamento de TI.

Entrevistado: Paola Solano - Analista de Negocio de TI

¿Cuáles son los problemas puntuales que se han presentado y que generan la necesidad de una certificación?

R/.

¿Cuál considera que es una preocupación principal de la empresa en temas de seguridad?

R/.

¿Se tiene establecida alguna estructura de caso de negocio por parte de la empresa que se deba implementar?

R/.

¿Se tienen estimados beneficios financieros esperados al obtener la certificación que deban ser tomados en cuenta?

R/.

Apéndice B. Entrevista con Analista de Negocio de CRM.

Entrevista 2

Fecha: 29/06/2021

Objetivo de la entrevista: Determinar los problemas presentados por el Departamento de TI.

Entrevistado: Javier Araya - Analista de Negocio CRM

¿Cuáles considera que son las causas del problema presentado en la empresa en la necesidad de una certificación?

R/

¿Considera que una de las causas es la falta de recursos humanos que se encarguen de garantizar la correcta gestión de la seguridad de la información?

¿Se encuentran trabajos o esfuerzos previos dentro de la organización en materia de seguridad de la información?

R/.

¿Cree usted que la resistencia al cambio podría ser un factor que afecte el proyecto?

R/.

Apéndice C. Grupos Focales.

Tabla C1. Grupo Focal 1.

Grupo Focal:	1	**Fecha:**	06/09/2021
Tema:	Determinar criterios de evaluación de brechas		
Lugar:	Microsoft Teams	**Total de participantes:**	3
Asistentes:	Paola Solano, Javier Araya y Bryan Blanco		
Preguntas de discusión			
¿Cuál podría ser el método de evaluación para el nivel de cumplimiento de cada área de control? ¿Cuál podría ser el método de priorización de las brechas identificadas según el cumplimiento de cada área de control?			
Resultados			
Determinar la calificación total por área de control de acuerdo al estado actual y la cantidad de controles de cada área. Fórmula de ponderación para determinar el nivel de cumplimiento por área de control y la priorización de las mismas.			

Tabla C2. Grupo Focal 2.

Grupo Focal:	2	**Fecha:**	11/10/2021
Tema:	Determinar factores críticos de éxito		
Lugar:	Microsoft Teams	**Total de participantes:**	4
Asistentes:	Juan José Mena, Paola Solano, Javier Araya y Bryan Blanco		
Preguntas de discusión			
¿Cuáles consideran que son los factores críticos de éxito del proyecto?			
Resultados			
• **Disponibilidad e interés del responsable o equipo ejecutor:** se deben asignar los responsables o equipo de trabajo dedicado a realizar las diferentes actividades. • **Mercado:** mejorar el posicionamiento en el mercado a través de un proceso de gestión de la seguridad de la información • **Eficiencia:** agilizar los procesos y operaciones en la organización, además de mantener los ambientes con la seguridad adecuada • **Anticipación:** la diversidad de industrias a las que pertenecen los clientes de la empresa y el creciente número de ataques informáticos preocupan a la organización y aumentan la rigurosidad en los requerimientos recibidos. • **Formación y capacitación:** Mantener a los usuarios del SGSI debidamente capacitados para garantizar la correcta implementación y monitorización del sistema. • **Concientización:** Realizar los programas de concientización permite que los colaboradores de la organización comprendan la importancia que tiene preservar la seguridad de la información en todos los procesos de negocio.			

Apéndice D. Verificación del método de observación aplicado.

Lista de verificación para la aplicación de la observación como instrumento para determinar el cumplimiento de controles en la infraestructura de TI de la organización.

A continuación se especifican los aspectos observados y evaluados a partir de la verificación realizada en las oficinas de Mobilize.Net.

Fecha: 24/08/2021

Verificaciones en el área de: Administración de activos

Controles	Verificación	Comentarios
Inventario	✓	Identificado, registrado y almacenado adecuadamente.
Etiquetado de los activos	X	Solo se realiza para algunos equipos

Verificaciones en el área de: Seguridad física y ambiental

Controles	Verificación	Comentarios
Perímetro físico de seguridad	✓	Perímetros claramente definidos
Controles de ingreso físicos	✓	Control por medio de credencial.
Aseguramiento de oficinas, salas e instalaciones.	✓	Áreas de trabajo identificadas y divididas adecuadamente.
Protección contra amenazas externas y ambientales	✓	Edificio y oficinas con sistemas certificados y recursos de prevención y protección contra amenazas.
Trabajo en áreas seguras	✓	Protocolos de trabajo con espacios definidos
Áreas de carga y entrega	✓	Ubicadas en la parte trasera del edificio.
Ubicación y protección del equipo	✓	Correcta ubicación de los equipos
Instalaciones de suministro	✓	Planta generadora de energía en caso de corte eléctrico.

Seguridad del cableado	✓	Protección adecuada del cableado por canaletas y racks.
Política de escritorio y pantalla limpios	✓	Bloqueo programado por inactividad, con política de directivas de grupo y escritorios limpios.

Verificaciones en el área de: Seguridad de la información en la gestión de la continuidad del negocio

Planificación de la continuidad de la seguridad de la información	✓	Respaldos de información y redundancia de sistema eléctrico a través de UPS y planta generadora. Se cuenta con una red de internet principal y una secundaria.

Apéndice E. Indicadores Clave de Rendimiento del Departamento de TI.

Objetivo del departamento	Rol	Objetivo del responsable	Descripción	Indicador
Enviar proyectos de clientes a tiempo y con calidad	Asesor de TI	Organización de TI	Ejecutar la estrategia en nuestra pila de tecnología de TI, como lo es, seguridad, continuidad del negocio y ejecución.	Dashboard del proyecto, reportes financieros del proyecto, plan de entrega del proyecto, plan de ejecución del proyecto, informe LoC / h
		Eficiencia en la ejecución	Buscar continuamente formas de optimizar la eficiencia en los procesos de trabajo y asegurándose de evitar cualquier tipo de regresiones.	Al menos el 95% de las tareas / asignaciones individuales se completaron sin regresiones ni errores informados por el cliente debido a nuevas implementaciones.
	Analista de negocio	Seguridad	Crear mecanismos para mejorar las medidas de seguridad y la IP de clientes.	Soluciones inteligentes para asegurar a nuestros clientes y potenciales clientes que sus datos están seguros con nosotros. Definir metodologías específicas para brindar esta información al cliente de una manera ágil y salir de cualquier tecnología heredada en los servicios que brindamos. Obtener comentarios de clientes o auditorías de clientes para implementar en nuestra organización, busque cosas pequeñas que generen el mayor impacto.

Objetivo del departamento	Rol	Objetivo del responsable	Descripción	Indicador
Satisfacción de clientes	Analista de negocio	Ejecución	Asegurar la ejecución de manera oportuna, priorizar contra la criticidad y el impacto.	Satisfacción del cliente. Mejora de la cobertura de tecnologías. Proporcione soluciones listas para usar para problemas complejos. Coordinar recursos para lograr resultados (ALBATROS). Gestión de hardware en todas las organizaciones.

Apéndice F. Identificación de Requerimientos de Clientes.

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.

#	Domain	Question	Comment	Evidence attached?
A. Risk Assessment				**Yes/No**
A.1	A. Risk Assessment	Is there a risk assessment program that has been approved by senior management; communicated to stakeholders, and reviewed periodically?		
A.2	A. Risk Assessment	Are risks to the organisation's information and information processing facilities from business processes involving external parties and customers identified, and are appropriate controls implemented before granting access?		
A.3	A. Risk Assessment	Does your organisation hold Commercial General Liability Insurance? (If yes, please specify per occurrence and aggregate limits or attach copy of certificate)		
A.4	A. Risk Assessment	Do you currently have Professional Liability Insurance Coverage? (If yes, please specify the limit or attach copy of certificate)		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
A.5	A. Risk Assessment	Is Network Security & Privacy Insurance Coverage held by your organisation? (If yes, please specify the limit or attach copy of certificate)		
B. Security Policy				
B.1	B. Security Policy	Is there an information security policy document that has been approved by senior management; communicated to all employees, and relevant external parties? (If so, please supply a copy)		
B.2	B. Security Policy	Is this information security policy reviewed periodically to ensure its continued suitability, adequacy, and effectiveness?		
C. Information Security Governance				
C.1	C. Information Security Governance	Are confidentiality or non-disclosure agreements designed and reviewed to reflect the organisation's own needs for protection of information, and meet all applicable laws, regulations, and commitments?		
C.2	C. Information Security Governance	Is a periodic independent review of information security management conducted? ***(Please attach any independent audit review reports or certifcations)***		
C.3	C. Information Security Governance	In provision of services, does your organisation utilize employees, subcontractors or third-party vendors from outside of the European Union that can access, process, communicate, store or manage Confluence or Confluence client information originating from this jurisdiction? (Please specify each country outside the European Union, indicating categories of processing, purpose and type of access; resources affected, and general description of technical and organisational measures (if possible)		
D. Asset Management				

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
D.1	D. Asset Management	Is there an asset management policy in place and communicated to all relevant parties? ***(Please attach a copy)***		
D.2	D. Asset Management	Are all assets clearly identified, and is there an inventory of important assets that is maintained and have owners assigned?		
D.3	D. Asset Management	Is asset destruction logged?		
D.4	D. Asset Management	Have the rules for the acceptable use of information and assets associated with information processing facilities been identified, documented, and implemented?		
D.5	D. Asset Management	Is there an information classification scheme in place?		
E. Human Resources Security				
E.1	E. Human Resources Security	Are security roles and responsibilities of employees and contractors defined and documented in accordance with the organisation's information security policy?		
E.2	E. Human Resources Security	Are background checks performed on employees and contractors before they are granted access to data?		
E.3	E. Human Resources Security	As part of their contractual obligation do all employees and contractors agree to and sign the terms and conditions of their employment contract, which state their and the organisation's responsibilities for information security?		
E.4	E. Human Resources Security	Are employees and contractors required to complete a security awareness training?		
E.5	E. Human Resources Security	Is there a formal disciplinary process for employees and contractors who are in breach of your organisation's or Confluence information?		
F. Physical and Environmental Security				

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
F.1	F. Physical and Environmental Security	Are critical or sensitive information processing facilities housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls?		
F.2	F. Physical and Environmental Security	Are critical or sensitive information processing facilities and equipment protected from environmental threats (fire, flood, earthquake, explosion, civil unrest, and other natural or man-made disaster), power failures and other disruptions caused by failures in supporting utilities?		
G. Communications and Operations Management				
G.1	G. Communications and Operations Management	Is there a change management policy in place?		
G.2	G. Communications and Operations Management	Is antivirus deployed to all types of servers and devices?		
G.3	G. Communications and Operations Management	Are systems and software automatic updates enabled for all provisioned devices?		
G.4	G. Communications and Operations Management	Is a firewall rule policy in place?		
G.5	G. Communications and Operations Management	Does your organisation carryout regular vulnerability scanning of Production environment(s)?		
G.6	G. Communications and Operations Management	Is a server hardening standard in place?		
G.7	G. Communications and Operations Management	Are user access logs enabled?		
G.8	G. Communications and Operations Management	Are admin activity logs enabled?		
G.9	G. Communications and Operations Management	Is a removable media (USB, CD etc.) policy in place?		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
G.10	G. Communications and Operations Management	Is use of removable media prohibited on in scope devices?		
G.11	G. Communications and Operations Management	Are users restricted from installing software without approval?		
G.12	G. Communications and Operations Management	Is an encryption policy in place?		
G.13	G. Communications and Operations Management	Is all data encrypted in transit?		
G.14	G. Communications and Operations Management	Is all data encrypted at rest?		
G.15	G. Communications and Operations Management	Is a real time Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) in place to monitor / protect all Internet connections?		
G.16	G. Communications and Operations Management	Is a bring your own device (BYOD) policy in place?		
H. Access Control				
H.1	H. Access Control	Is there an Access Management Policy in place to cover granting, changing and terminating access? ***(If so, please attach evidence)***		
H.2	H. Access Control	Is there a formal process for removal of the access rights of all employees, contractors and third party users to information and information processing facilities upon termination of their employment, contract or agreement, and return of all organizational assets in their possession?		
H.3	H. Access Control	Is the allocation and use of privileges restricted, controlled and periodically reviewed by management?		
H.4	H. Access Control	Is a central system used to manage access requests and approvals?		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
H.5	H. Access Control	Is segregation of duties enforced when requesting, approving and granting access?		
H.6	H. Access Control	Are all user IDs unique?		
H.7	H. Access Control	Are shared admin or super user accounts prohibited?		
H.8	H. Access Control	Is unauthorized access to operating systems prevented using authenticating authorized users, password management system, session time-outs and other security measures?		
H.9	H. Access Control	Is a password policy in place. Please detail settings? ***(If so, please attach evidence)***		
H.10	H. Access Control	Are password requirements detailed in the policy technically enforced (minimum character length, complexity requirements)?		
H.11	H. Access Control	Is a remote access policy in place?		
H.12	H. Access Control	Are local admin rights disabled on staff provisioned devices?		
I. Information Systems Application Development and Maintenance				
I.1	I. Information Systems Application Development and Maintenance	Is policy on the use of cryptographic controls for protection of information developed and implemented, and is key management in place to support the use of cryptographic techniques?		
I.2	I. Information Systems Application Development and Maintenance	Is a software development life cycle (SDLC) policy in place? Does it comply with any applicable regulatory requirements such as General Data Protection Regulation (GDPR) or any other relevant data privacy law?		
I.3	I. Information Systems Application Development and Maintenance	Are the development, test and production environments segregated?		
I.4	I. Information Systems Application Development and Maintenance	Is outsourced software development supervised and monitored by the organisation?		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
J. Information Security Incident				
J.1	J. Information Security Incident	Is an incident management policy in place? ***(If so, please attach evidence)***		
J.2	J. Information Security Incident	Is a centralized system in place to manage incidents and track through remediation?		
J.3	J. Information Security Incident	If there is an incident that impacts clients, how is this communicated?		
K. Business Continuity and Disaster Recovery				
K.1	K. Business Continuity and Disaster Recovery	Is a business continuity policy in place? ***(If so, please attach evidence)***		
K.2	K. Business Continuity and Disaster Recovery	Are the Business Continuity and Disaster Recovery plans tested annually?		
K.3	K. Business Continuity and Disaster Recovery	Are back up tapes stored offsite?		
K.4	K. Business Continuity and Disaster Recovery	Are fire safety controls in place to prevent and contain a fire in the data centre? Are environmental controls in place to manage the risk of damage to data centre in the event of a disaster?		
K.5	K. Business Continuity and Disaster Recovery	Is sufficient power supply available for the data centre if the main supply were unavailable?		
L. Compliance				
L.1	L. Compliance	Does your company carry out documented risk assessments of its business and supply chain to ensure continuous compliance with relevant statutory requirements? ***(Supplier should provide evidence to confirm that appropriate administrative, technical, and physical controls are in place to***		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
		conform with all relevant legislative, statutory, regulatory, and contractual requirements)		
L.2	L. Compliance	Does your company have a regularly monitored anti-corruption code of conduct documenting your anti-corruption and bribery policies and procedures?		
L.3	L. Compliance	Is this anti-corruption code of conduct known and acted upon by all employees of your company?		
L.4	L. Compliance	Is this anti-corruption code of conduct publicised internally and externally?		
L.5	L. Compliance	Does your company carry out documented risk assessments of its potential exposure to corruption and bribery?		
L.6	L. Compliance	Does your company apply due diligence procedures for persons who perform or will perform services for or on behalf of the organisation, to mitigate identified bribery risks?		
L.7	L. Compliance	Is your company required by section 54 of the UK's Modern Slavery Act to produce an annual statement setting out the steps that have been taken to ensure your company and supply chains are slavery free?		
L.8	L. Compliance	Does your company have a policy on modern slavery and human trafficking? (this may form part of your company's wider CSR policy)		
M. Privacy				
M.1	M. Privacy	Does your system involve the collection of information about individuals?		

The quetsionnaire should be distributed to relevant subject matter experts (SME) from the service provider to ensure each question is answered accurately.				
#	**Domain**	**Question**	**Comment**	**Evidence attached?**
M.2	M. Privacy	Does your system involve the use of new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		
M.3	M. Privacy	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.		
M.4	M. Privacy	Will your system require you to contact individuals in ways that they may find intrusive?		
M.5	M. Privacy	Is a privacy policy in place? ***(If so, please attach evidence)***		
M.6	M. Privacy	Is a process in place to notify clients and regulators in the event of a breach?		
M.7	M. Privacy	Are safeguards in place to ensure compliance with relevant country or regional laws regarding cross-border transfer of information?		
N. Third Party				
N.1	N. Third Party	Is a third party risk management policy in place?		
N.2	N. Third Party	For each risk identified, has a risk treatment decision been taken?		
N.3	N. Third Party	Are contracts in place with all third parties?		
N.4	N. Third Party	Is an NDA in place with all vendors?		
O. Cloud - (if applicable)				
O.1	O. Cloud	Is a cloud computing policy in place?		
O.2	O. Cloud	Is your instance configured as a private subnet to segregate your data from other customers?		
O.3	O. Cloud	Is the cloud encryption key managed by your company?		

Apéndice G. Políticas, Controles y Procedimientos de la Norma ISO 27002:2013 Propuestos.

G.1. Cadena de suministro de tecnología de información y de las comunicaciones

Control: Se deben incluir los requerimientos necesarios para hacer frente a los riesgos de seguridad de la información relacionados con la cadena de suministro de las tecnologías de información y comunicación (TIC) (International Organization for Standardization, 2013b).

Se recomienda tomar en cuenta los siguientes aspectos para definir la política y los acuerdos en la cadena de suministro con los proveedores de la organización.

- Definir los requerimientos de seguridad de la información que apliquen al momento de realizar compras de servicios de TIC y las relaciones con proveedores.
- En aquellos casos que el proveedor subcontrate partes de los servicios o compre componentes de las TIC que se suministran a la organización a otros proveedores, se debe garantizar que los requerimientos establecidos para la seguridad de la información sean reproducidos a lo largo de la cadena de suministro.
- Definir procesos y métodos para supervisar que los productos y servicios de TIC adquiridos cumplan con los requerimientos de seguridad de la información establecidos.
- Identificar los componentes de productos y servicios que son críticos para su funcionamiento de forma que se pueda mantener un mayor control al momento de su construcción, principalmente cuando el proveedor subcontrata partes o componentes del producto o servicios a otros proveedores.
- Verificar que se garantice la trazabilidad de los componentes críticos a lo largo de la cadena de suministro.

- Verificar el correcto funcionamiento esperado de los productos de TIC suministrados.
- Definir reglas para el intercambio de información con respecto a la cadena de suministro y la gestión de posibles problemas y compromisos adquiridos entre la organización y proveedores.
- Implementar procesos específicos para la gestión de la información y el ciclo de vida, además de la disponibilidad y los riesgos de la seguridad de la información asociados a los componentes de TIC. Se deben incluir los riesgos por cese de operaciones o la ausencia de disponibilidad de los componentes por obsolescencia.

G.2. Gestión de cambios en servicios con proveedores

Control: Se deben gestionar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de políticas, procedimientos y controles de seguridad de la información actuales, tomando en cuenta el nivel de criticidad de los sistemas y procesos de negocio que se pueden ver afectados (International Organization for Standardization, 2013b).

Se recomienda tomar en cuenta los siguientes aspectos para definir la política y los acuerdos en la gestión de cambios con los proveedores de la organización.

- Cambios en los acuerdos con proveedores
- Nuevas implementaciones en la organización que provoquen cambios relacionados con:
- Mejoras en servicios actuales.
- Desarrollo de nuevos sistemas o aplicaciones.
- Modificación o actualización de políticas o procedimientos en la organización.

- Nuevos controles enfocados en la mejora de la seguridad de la información relacionada con incidentes.
- Nuevas implementaciones en los servicios de proveedores que provoquen cambios relacionados con:
    - Cambios y mejoras en las redes.
    - Nuevas tecnologías.
    - Introducción de nuevos productos o versiones.
    - Nuevas herramientas y entornos de desarrollo.
    - Cambio de ubicación física de las instalaciones de servicio.
    - Cambio de proveedores.
    - Subcontratación a otro proveedor.

G.3. Clasificación de la información

Control: La información debe ser clasificada de acuerdo a su importancia de revelación frente a requerimientos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas (International Organization for Standardization, 2013b).

La organización debe considerar los siguientes aspectos para establecer las políticas relacionadas con la clasificación de la información.

- Considerar las necesidades de negocio al compartir o restringir información, así como los requisitos legales relacionados.
- Los activos deben ser clasificados de acuerdo a la clasificación de la información que almacenan o procesan.
- El nivel de protección en el esquema de clasificación debe considerar los criterios de confidencialidad, integridad y disponibilidad de la información.
- Los propietarios de los activos deben ser responsables de su clasificación.

- El esquema de clasificación debe ser consistente en toda la organización de manera que todas las personas clasifiquen los activos y la información de la misma forma y se tenga un entendimiento en común de los requerimientos de protección y sean aplicados de la manera adecuada.
- Los valores de la clasificación deben actualizarse en el momento que cambien sus valores, sensibilidad o criticidad de los activos a lo largo del ciclo de vida.

G.4. Etiquetado de la información

Control: debe desarrollarse e implementarse un conjunto adecuado de procedimientos que permitan el etiquetado de la información de acuerdo al esquema de clasificación establecido por la organización (International Organization for Standardization, 2013b).

Se deben tomar en cuenta los siguientes aspectos que permitan definir una política para el adecuado etiquetado de la información.

- Los procedimientos de etiquetado de la información deben contemplar los activos de información tanto físicos como electrónicos.
- El proceso de etiquetado se debe establecer de acuerdo con el esquema de clasificación definido por la organización.
- Las etiquetas deben ser fácilmente reconocibles.
- Se deben establecer directrices sobre dónde y cómo se vinculan las etiquetas según la manera en que se accede a la información o cómo se tratan los activos dependiendo de su tipo.
- Se pueden definir los casos en que sea posible prescindir del etiquetado de la información para activos no confidenciales de forma que se reduzca la carga de trabajo.

- Concientizar sobre el proceso de etiquetado tanto a empleados como externos de la organización.
- Se debe incluir el etiquetado de los resultados producidos por sistemas que contengan información crítica o sensible para la organización.

G.5. Gestión de medios extraíbles

Control: Se deben implementar procedimientos que garanticen la gestión de medios extraíbles de acuerdo con los criterios de clasificación de la información definidos por la organización (International Organization for Standardization, 2013b).

Se recomienda tomar en cuenta los siguientes aspectos para definir la política en la gestión de medios extraíbles de la organización.

- Eliminar definitivamente todo contenido que ya no sea necesario de cualquier medio reutilizable que vaya a ser eliminado.
- Evaluar las situaciones en las que sea práctico y necesario solicitar autorización para extraer medios de la organización y mantener el registro adecuado de la trazabilidad para efectos de la auditoría.
- Almacenar los medios en un entorno seguro de acuerdo a las recomendaciones del fabricante.
- Encriptar los datos contenidos en medios extraíbles de acuerdo a los criterios de confidencialidad e integridad definidos.
- Transferir los datos de medios que se encuentran pronto a cumplir su vida útil hacia nuevos medios de forma que se mitiguen los riesgos por ilegibilidad o daño de la información almacenada.
- Almacenar copias de la información crítica en diferentes medios para mitigar los riesgos por daño o pérdida simultánea de información.

- Considerar el inventario de medios para limitar y controlar la pérdida de datos
- Permitir la reproducción del contenido en medios extraíbles únicamente cuando exista una razón de negocio.
- Monitorizar la transferencia de medios extraíbles cuando sea requerido.

G.6. Eliminación de medios extraíbles

Control: Se deben eliminar los medios extraíbles mediante procedimientos adecuados y de forma segura en el momento que estos ya no vayan a ser necesarios (International Organization for Standardization, 2013b).

Se recomienda tomar en cuenta los siguientes aspectos para definir la política en la eliminación de medios extraíbles de la organización.

- Se deben almacenar y desechar de manera segura aquellos medios extraíbles que contengan información confidencial de la organización, así como eliminar dicha información en caso de reutilizar el medio.
- Implementar procedimientos para identificar los medios extraíbles que requieran de una eliminación segura.
- Evaluar la necesidad de encargar a terceros con la experiencia y controles necesarios la eliminación segura de los medios.
- Registrar la eliminación de medios críticos o sensibles que brinden la trazabilidad requerida para efectos de la auditoría.

G.7. Transporte de medios extraíbles

Control: Se deben proteger contra accesos no autorizados, uso inadecuado o deterioro a todo medio extraíble durante el transporte fuera de los límites físicos de la organización (International Organization for Standardization, 2013b).

Se recomienda tomar en cuenta los siguientes aspectos para definir la política en el transporte de medios extraíbles de la organización.

- Emplear un servicio fiable de transporte o mensajería.
- Acordar con la alta dirección una lista de mensajeros autorizados.
- Definir procedimientos para verificar la identidad de los mensajeros.
- El embalaje debe brindar la protección ante factores externos que pueden afectar el contenido según las especificaciones de su fabricante.
- Mantener un registro e identificación del contenido y protección aplicada, así como una bitácora con los momentos de entrega al mensajero y recepción en el destino.

G.8. Contacto con las autoridades

Control: Se debe adoptar una política y medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles (International Organization for Standardization, 2013b).

Para definir la política de dispositivos móviles se deben considerar los siguientes aspectos.

- Asegurar que no se compromete información crítica del negocio con el uso de dispositivos móviles.
- Identificar y evaluar los riesgos presentados por el uso de dispositivos móviles en ambientes desprotegidos.
- Registrar el dispositivo móvil.
- Definir los requerimientos para la protección física del dispositivo.
- Restricciones en la instalación de software

- Requerimientos de versiones de software para la aplicación de parches y actualizaciones.
- Restricciones en las conexiones con servicios de información.
- Definir los controles de acceso.
- Definir las técnicas criptográficas aplicables.
- Establecer la protección adecuada contra software malicioso.
- Establecer mecanismos de inhabilitación, eliminación y bloqueos remotos.
- Mantener copias de respaldo.
- Consideraciones en la utilización de servicios y aplicaciones web.

G.9. Política en el uso de controles criptográficos

Control: Se debe definir e implementar una política sobre el uso de controles criptográficos para proteger la información (International Organization for Standardization, 2013b).

Para desarrollar la política la organización debe tener en cuenta los siguientes aspectos.

- Definir el enfoque de la Dirección con respecto al uso de controles criptográficos en toda la organización de acuerdo a los principios establecidos para proteger la información de negocio.
- Se debe tomar en cuenta la evaluación de los riesgos y el nivel de protección necesario para establecer el tipo, fortaleza y calidad del algoritmo requerido.
- Se deben establecer métodos para la protección adecuada de claves criptográficas y la recuperación de la información cifrada en caso de pérdida o daño de las claves.
- Definir las funciones y responsables de la implementación de la política y la gestión de las claves incluyendo la generación de las mismas.

- Definir la solución que debe adoptar cada proceso de negocio para la correcta implementación en toda la organización.
- Identificar el posible impacto que pueda generar la información cifrada en los controles que requieran inspección del contenido en la detección de malware.
- Tomar en cuenta las regulaciones y restricciones nacionales que puedan aplicar al uso de técnicas criptográficas en los países de interés para la organización, así como aspectos relacionados al envío de información transfronteriza.
- Establecer los controles criptográficos necesarios para garantizar la confidencialidad e integridad de la información en su almacenamiento y transferencia de acuerdo a los criterios establecidos en la clasificación de la información.

G.10. Gestión de claves

Control: se debe desarrollar e implementar una política sobre el uso, protección y duración de las claves de cifrado a lo largo de su ciclo de vida (International Organization for Standardization, 2013b).

Para desarrollar la política la organización debe tener en cuenta los siguientes aspectos.

- Establecer los requisitos para la adecuada gestión de claves criptográficas en todo su ciclo de vida, incluyendo la generación, almacenamiento, registro, recuperación, distribución, retiro y eliminación de las mismas.

- Establecer medidas de protección contra la modificación, pérdida o eliminación de las claves criptográficas, así como su posible revelación no autorizada, tomando en cuenta la seguridad física de los equipos que contienen las mismas.

- Generar las claves necesarias para los distintos sistemas y aplicaciones.
- Generar y obtener los certificados de clave pública.
- Distribuir adecuadamente las claves a los respectivos usuarios y establecer la forma en que deben ser utilizadas.
- Almacenar adecuadamente las claves con los controles para el acceso autorizado respectivos.
- Acciones ante claves comprometidas.
- Definir el proceso para la revocación de claves.
- Definir el proceso para la recuperación de claves perdidas o corruptas.
- Mantener el registro y las copias de respaldo de las claves.
- Definir el proceso para la eliminación de claves.
- Registrar y auditar las actividades relacionadas con la gestión de claves.

G.11. Disponibilidad de los recursos de tratamiento de la información

Control: los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad (International Organization for Standardization, 2013b).

La organización debe identificar adecuadamente los requerimientos de disponibilidad para los sistemas de información. En caso que la disponibilidad no pueda

ser garantizada a través de la arquitectura de los sistemas existentes se deben evaluar los componentes o arquitecturas de redundancia necesarios.

Apéndice H. Matriz de Evaluación de la Seguridad de la Información.

Estado Actual	Descripción
3	Se aplican las acciones adecuadas y se cumple con los requerimientos en el control.
2	Se realizan algunas acciones pero existen oportunidades de mejora o necesidades para cumplir con los requerimientos en el control.
1	No se aplican las acciones requeridas para cumplir con los requerimientos en el control.
N/A	El control no aplica de acuerdo a las políticas de la organización.

Evaluación de Seguridad de la Información ISO/IEC 27001:2013

Área de control	Control	Sí	No	N/A	Documentación	Controles existentes	Observaciones	Fase de Identificación	Estado actual
1	**Políticas en seguridad de la información**								
Dirección de gestión para la	Políticas para la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

seguridad de la información	Revisión de las políticas para la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
2	**Organización de la seguridad de la información**								
Organización interna	Roles y responsabilidades en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Segregación de deberes	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Contacto con las autoridades		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Contacto con grupos de interés especiales	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Seguridad de la información en la administración de proyectos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Dispositivos móviles y teletrabajo	Política de dispositivos móviles	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Teletrabajo	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
3	**Seguridad de los recursos humanos**								

Previo al empleo	Proyección	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Términos y condiciones del empleo	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Durante el empleo	Administración de responsabilidades	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Concientización, educación y capacitación en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Proceso disciplinario	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
Finalización y cambio del empleo	Finalización o cambio de responsabilidades laborales	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
4	**Administración de activos**								
Responsabilidad de los activos	Inventario de activos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Propiedad de los activos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Uso adecuado de los activos	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Devolución de los activos	x						Análisis de estándar ISO 27001 e ISO 27002	**2**

Clasificación de la información	Clasificación de la información		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Etiquetado de información		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Manejo de los activos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Manejo de los medios	Gestión de medios extraíbles		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Eliminación de los medios		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Transporte de medios físicos		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
5	**Control de accesos**								
Requerimientos del negocio en controles de acceso	Política de control de accesos	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Acceso a redes y servicios de red	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Gestión del acceso de usuarios	Registro y deshabilitación de usuarios	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Aprovisionamiento de acceso a usuarios	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

	Gestión de derechos de acceso privilegiado	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Gestión de la información secreta de autenticación de usuarios	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Revisión de los derechos de acceso de los usuarios		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Eliminación y ajustes de los derechos de acceso	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Control de accesos a sistemas y aplicaciones	Uso de la información secreta de autenticación de usuarios	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Restricciones de acceso a la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Procedimientos de inicio de sesión seguros	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Sistema de gestión de contraseñas	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Uso privilegiado de los programas de utilidad	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Control de acceso a código fuente de programas	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
6	**Criptografía**								

Controles criptográficos	Políticas en el uso de controles criptográficos	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Gestión de claves	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
7	**Seguridad física y ambiental**								
Áreas seguras	Perímetro físico de seguridad	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Controles de ingreso físicos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Aseguramiento de oficinas, salas e instalaciones.	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Protección contra amenazas externas y ambientales	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Trabajo en áreas seguras	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Áreas de carga y entrega	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Equipo	Ubicación y protección del equipo	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Instalaciones de suministro	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

	Seguridad del cableado	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Mantenimiento del equipo	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Retiro de activos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Seguridad de equipo y activos fuera de las instalaciones	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Eliminación o reutilización segura de equipos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Equipo de usuario desocupado	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Política de escritorio y pantalla limpios	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
8	**Seguridad de las operaciones**								
Procedimientos y responsabilidades operacionales	Documentación de procedimientos operativos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Gestión del cambio	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Gestión de la capacidad	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

	Separación entre entornos de desarrollo, pruebas y operativos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Protección contra malware	Controles contra malware	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Copias de seguridad	Respaldos y copias de seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Registro y control	Registro de eventos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Protección de la información de registro	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Registros de administrador y operador	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Sincronización de tiempo	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Control de software operativo	Instalación de software en sistemas operativos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Gestión de vulnerabilidades técnicas	Gestión de vulnerabilidades técnicas	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Restricciones en la instalación de software	x						Análisis de estándar ISO 27001 e ISO 27002	**2**

Consideraciones en la auditoría de sistemas de información	Controles de auditoría en sistemas de información		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
9	**Seguridad de las comunicaciones**								
Gestión de la seguridad de red	Controles de red	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Seguridad de los servicios de red	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Segregación en redes		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
Transferencia de información	Políticas y procedimientos para la transferencia de información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Acuerdos sobre la transferencia de información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Mensajería electrónica	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Acuerdos de confidencialidad y no divulgación	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
10	**Adquisición, desarrollo y**								

	mantenimiento de sistemas								
Requerimientos de seguridad de sistemas de información	Análisis y espcificación de requerimentos en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Protección de los servicios de aplicaciones en redes públicas	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Protección de transacciones en servicios de aplicaciones	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Seguridad en procesos de desarrollo y soporte	Política de desarrollo seguro	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Procedimientos de control de cambios del sistema	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Revisión técnica de aplicaciones después de cambios de plataforma operativa	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Restricciones sobre cambios en paquetes de software	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Principios de ingeniería de sistemas seguros	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Entorno de desarrollo seguro	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

	Desarrollo subcontratado	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Pruebas de seguridad del sistema	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Pruebas de aceptación del sistema	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Datos de prueba	Protección de los datos de prueba	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
11	**Relación con proveedores**								
Seguridad de la información en las relaciones con proveedores	Política de seguridad de la información para las relaciones con proveedores		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
	Abordar la seguridad dentro de los acuerdos con proveedores	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Cadena de suministro de las tecnologías de información y comunicación		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
Gestión de los servicios de proveedores	Control y revisión de los servicios de proveedores	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Gestión de cambios en los servicios de proveedores		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
12	**Gestión de incidentes de**								

	seguridad de la información								
	Responsabilidades y procedimientos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Informe de eventos en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Informe de debilidades en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Evaluación y decisión de eventos en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Respuesta a incidentes en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Aprendizaje de los incidentes en seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
	Recolección de evidencia	x						Análisis de estándar ISO 27001 e ISO 27002	**2**
13	**Seguridad de la información en la gestión de la continuidad del negocio**								
Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

	Implementar la continuidad de la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Verificar, revisar y evaluar la continuidad de la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Redundancias	Disponibilidad de los recursos de tratamiento de la información		x					Análisis de estándar ISO 27001 e ISO 27002	**1**
14	**Cumplimiento**								
Cumplimiento de requisitos legales y contractuales	Identificación de la legislación aplicable y los requisitos contractuales	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Derechos de propiedad intelectual	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Protección de los registros de la organización	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Privacidad y protección de la información de carácter personal	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Regulación de controles criptográficos	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
Revisiones de la seguridad de la información	Revisión independiente de la seguridad de la información	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
	Cumplimiento con políticas y estándares de seguridad	x						Análisis de estándar ISO 27001 e ISO 27002	**3**

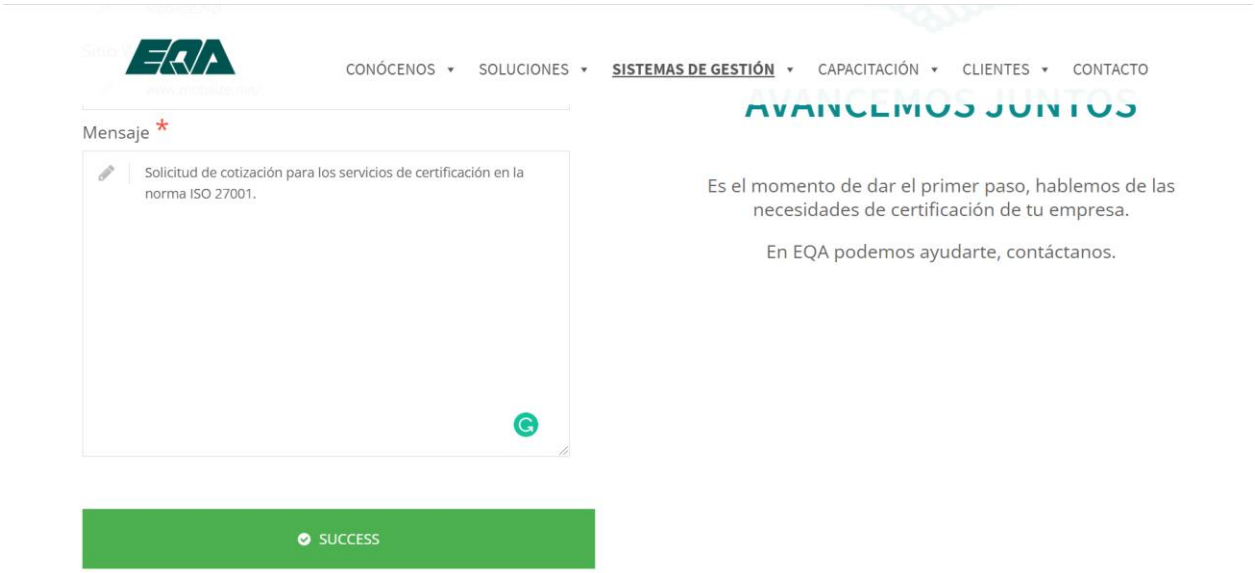
	Revisión de cumplimiento técnico	x						Análisis de estándar ISO 27001 e ISO 27002	**3**
15	**Gestión de riesgos**								
	¿Existe un proceso de gestión de riesgos documentado, alineado a la organización, con criterios definidos y debidamente aprobado por la dirección?		x					Requerimiento de clientes	**1**
	¿Se define un alcance que incluya objetivos, resultados esperados, tiempos, recursos y herramientas de evaluación para el proceso de gestión de riesgos?		x					Requerimiento de clientes	**1**
	¿Se definen los riesgos con sus criterios de aceptación de acuerdo a los objetivos de la organización y se identifacan las causas y consecuencias asociados a cada uno de los riesgos?		x					Requerimiento de clientes	**1**
	¿Se identifican los riesgos para la seguridad de la información para la organización y las instalaciones de procesamiento de información relacionados a procesos comerciales, partes externas o clientes y se implementan los controles	x						Requerimiento de clientes	**2**

	adecuados antes de otorgar acceso?								
	¿Se encuentran controles para cada riesgo debidamente clasificados en: predicción, prevención, detección y corrección?		x					Requerimiento de clientes	**2**
	¿Se cuenta con escenarios establecidos en los que se identifiquen los diferentes eventos, las amenazas y los activos que se pueden ver afectados?		x					Requerimiento de clientes	**1**
	¿La organización cuenta con un seguro de responsabilidad comercial general?		x					Requerimiento de clientes	**1**
	¿La organización tiene actualmente cobertura de seguro de responsabilidad profesional?		x					Requerimiento de clientes	**1**
	¿Se cuenta con un responsable del proceso a cargo del plan de acción, plan de respuesta y actualización de la gestión?	x						Requerimiento de clientes	**1**
	¿Se realizan las revisiones al proceso periódicamente?		x					Requerimiento de clientes	**1**

16	**Privacidad**								
	¿El sistema implica la recopilación de datos personales de los usuarios?	x						Requerimiento de clientes	**3**
	¿La información personal es revelada o retenida por terceros?			x				Requerimiento de clientes	**N/A**
	¿Se cuenta con una política de privacidad establecida?	x						Requerimiento de clientes	**3**
	¿Existen salvaguardias para garantizar el cumplimiento de las leyes nacionales o regionales pertinentes con respecto a la transferencia transfronteriza de información?	x						Requerimiento de clientes	**3**
17	**Tercerización**								
	¿Existe una política para la gestión de riesgo relacionados a terceras partes?		x					Requerimiento de clientes	**1**
	¿Se encuentran los contratos relacionados a terceras partes debidamente documentados?	x						Requerimiento de clientes	**3**
	¿Existe un acuerdo de confidencialidad con todos los proveedores?	x						Requerimiento de clientes	**3**
18	**Servicios en la nube**								
	¿Existe una política para la computación en la nube definida por la organización?		x					Requerimiento de clientes	**1**

	¿Su instancia está configurada como una subred privada para segregar sus datos de otros clientes?	x						Requerimiento de clientes	**3**
	¿La organización gestiona la clave de cifrado en la nube?	x						Requerimiento de clientes	**3**

Apéndice I. Cotización EQA.



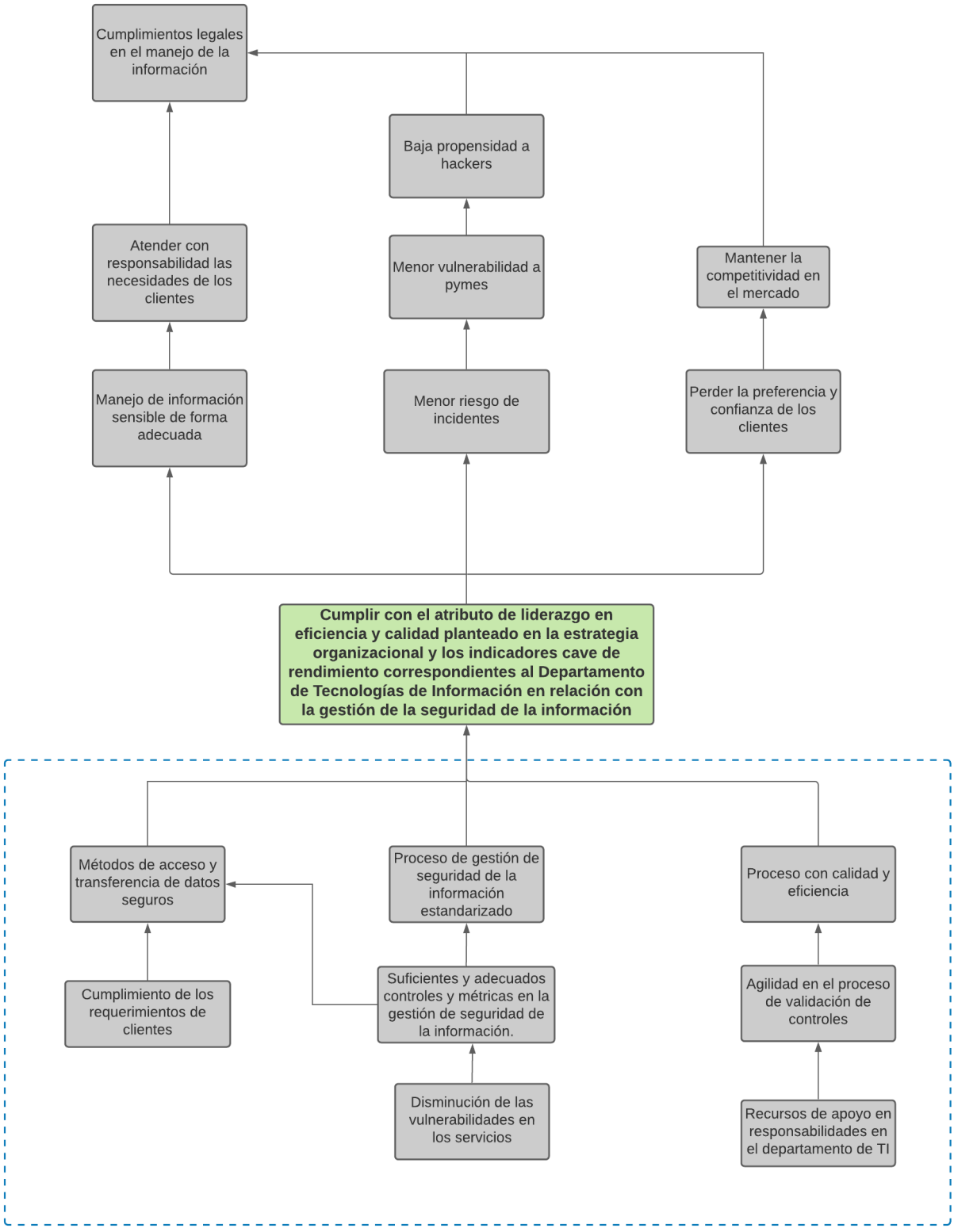
Apéndice J. Cotización BSI Group.

Apéndice K. Cotización INTECO.

Oferta

PRODUCTOS	CANTIDAD	FECHA ESTIMADA DEL PROCESO	IMPUESTOS	PRECIO POR UNIDAD	PRECIO TOTAL
Año 1					
Análisis documental	5.00 Día(s)	06/2022	Tarifa General 13%	1,100.00	$ 6,215.00
Evaluación de Cumplimiento	6.00 Día(s)	12/2022	Tarifa General 13%	1,100.00	$ 7,458.00
Emisión, mantenimiento o anualidad de Certificación	1.00 Otro tipo de servicios	01/2023	Tarifa General 13%	450.00	$ 508.50
				Subtotal:	**$ 14,181.50**
Año 2					
Auditoría de Seguimiento 1	4.00 Día(s)	10/2023	Tarifa General 13%	1,100.00	$ 4,972.00
Emisión, mantenimiento o anualidad de Certificación	1.00 Otro tipo de servicios	10/2023	Tarifa General 13%	450.00	$ 508.50
				Subtotal:	**$ 5,480.50**
Año 3					
Auditoría de Seguimiento 2	4.00 Día(s)	10/2024	Tarifa General 13%	1,100.00	$ 4,972.00
Emisión, mantenimiento o anualidad de Certificación	1.00 Otro tipo de servicios	10/2024	Tarifa General 13%	450.00	$ 508.50
				Subtotal:	**$ 5,480.50**
				Subtotal:	**$ 22,250.00**
				Impuestos:	$ 2,892.50
				Total:	**$ 25,142.50**

Apéndice L. Árbol de Objetivos.



Apéndice M. Minutas con Tutor

Tabla M1. Consulta de recomendaciones a tutor.

Reunión No.	04	**Fecha:**	01/07/2021
Lugar:	Microsoft teams	**Hora Inicio/Finalización:**	9:00 am. / 9:15 am
Objetivo de la reunión:	Consulta y recomendaciones		
Participantes:	Presentes: Carlos Mata, Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Consulta sobre recomendaciones en el documento de anteproyecto	Detallar que se incluirán los análisis necesarios. Enfocar en el estudio técnico. Diagrama de desarrollo del producto.	Realizar los cambios necesarios en el documento. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	**Fecha**	**Convocados**
Primeras indicaciones de la empresa	13/07/2021	Paola Solano, Javier Araya, Bryan Blanco

Tabla M2. Minuta de consulta a tutor.

Reunión No.	08	**Fecha:**	04/08/2021
Lugar:	Microsoft teams	**Hora Inicio/Finalización:**	05:00 pm. / 06:20 pm
Objetivo de la reunión:	Consulta a tutor		
Participantes:	Presentes: Carlos Mata, Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Confirmar el avance realizado en el análisis de la situación actual.	El tutor aprueba el avance realizado hasta el momento.	Se realizan los cambios y se adapta la estructura del árbol. Se aprueban los cambios por parte del tutor. Responsable: Bryan Blanco
2	Se analizan las posibles partes que llevará el caso de negocio.	Se brinda documento de referencia por parte del profesor.	Se consultará a la empresa si tienen alguna estructura establecida. Responsable: Bryan Blanco

3	Consulta por recomendaciones generales en el documento.	Se brindan las recomendaciones en el alcance, justificación e introducción del documento.	Se tomarán las recomendaciones y se aplicarán en el documento. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Consulta de seguimiento		10/08/2021	Carlos Mata y Bryan Blanco.

Tabla M3. Minuta de consulta a tutor.

Reunión No.	10	**Fecha:**	10/08/2021
Lugar:	Microsoft teams	**Hora Inicio/Finalización:**	05:00 pm. / 05:30 pm
Objetivo de la reunión:	Consulta a tutor		
Participantes:	Presentes: Carlos Mata, Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Definir la metodología de trabajo (por capítulos o por objetivos)	Tanto el tutor como el estudiante prefieren la metodología tradicional de entrega por capítulos.	Se trabajará el documento bajo la entrega por capítulos Responsable: Bryan Blanco
2	Se coordina la primera reunión entre estudiante, tutor y empresa.	Se establecen la hora y el día de la reunión.	Se programa la reunión por Microsoft Teams. Responsable: Bryan Blanco
3	Operacionalización de variables	Se revisará material de referencia brindado por el profesor para la operacionalización de variables como borrador de la metodología.	Se realizará un documento preliminar con la operacionalización de variables para el análisis de la situación actual de la empresa. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Siguiente consulta de seguimiento		11/08/2021	Carlos Mata y Bryan Blanco.

Tabla M4. Minuta de consulta a tutor.

Reunión No.	11	**Fecha:**	11/08/2021
Lugar:	Microsoft teams	**Hora Inicio/Finalización:**	17:00 pm. / 18:30 pm
Objetivo de la reunión:	Consulta a tutor		
Participantes:	Presentes: Carlos Mata, Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Consulta sobre los cambios realizados en el documento	Las adaptaciones realizadas se encuentran acorde a los indicadores de la empresa.	Cambios aprobados. Responsable: Carlos Mata
2	Dudas relacionadas al alcance	Pendiente de confirmar el alcance en la primera reunión con la empresa.	Definir y presentar las consultas a las partes. Responsable: Bryan Blanco
3	Operacionalización de variables del objetivo 1	Se establecen los atributos, la conceptualización, indicadores e instrumentos para el primer objetivo	Se tomarán las recomendaciones y se aplicarán en el documento. Responsable: Bryan Blanco
4	Revisión de documento Verificación de controles ISO 27001	Dudas generadas pendientes de revisar en el documento acerca de su evaluación.	Se consultará a la empresa y profesores correspondientes. Responsable: Bryan Blanco.

Próxima reunión		
Temas a tratar	**Fecha**	**Convocados**
Primer reunión con la empresa	12/08/2021	Paola Solano, Javier Araya, Carlos Mata y Bryan Blanco.

Tabla M5. Minuta de revisión de avance con tutor.

Reunión No.	13	**Fecha:**	19/08/2021
Lugar:	Microsoft teams	**Hora Inicio/Finalización:**	10:40 am. / 11:10 am
Objetivo de la reunión:	Consulta a tutor		
Participantes:	Presentes: Carlos Mata, Bryan Blanco		
	Ausentes:		
Temas Tratados			

No.	Asunto	Comentarios	Acuerdos
1	Consulta sobre los cambios realizados en el documento	Las adaptaciones realizadas se encuentran acorde a los indicadores de la empresa.	Cambios aprobados. Responsable: Carlos Mata
2	Alineación del problema con respecto a los indicadores del departamento	Se dan las recomendaciones por parte del tutor.	Aplicar los cambios acordados. Responsable: Bryan Blanco
3	Consulta por recomendaciones generales	Agregar párrafo antes de cita y adjuntar apéndice de los indicadores claves de éxito.	Se tomarán las recomendaciones y se aplicarán en el documento. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Inicio de capítulo II		25/08/2021	Carlos Mata y Bryan Blanco.

Tabla M6. Minuta de revisión de documento.

Reunión No.	14	**Fecha:**	19/08/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	16:30 pm. / 16:40 pm
Objetivo de la reunión:	Consulta sección ISO 27001		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Consulta por área de controles ISO 27001 Adquisición, desarrollo y mantenimiento de sistemas	Mantener la visión desde la infraestructura de TI sin entrar en detalles del desarrollo.	Realizar la verificación de acuerdo a lo acordado. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Seguimiento del avance		25/08/2021	Carlos Mata y Bryan Blanco

Tabla M7. Minuta de consulta de seguimiento con tutor.

Reunión No.	18	**Fecha:**	25/08/2021

Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	05:00 pm. / 06:25 pm
Objetivo de la reunión:	Consulta de seguimiento.		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Definir tipo de metodología	Se analizan las opciones de metodología expuestas en el taller con Luis Zeledón.	Se implementa una metodología tradicional para el proyecto. Responsable: Bryan Blanco
2	Se definen las secciones de la metodología	Se establecen los instrumentos y sujetos de investigación.	Se toman las notas y se documenta la operacionalización de variables. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	**Fecha**	**Convocados**
Análisis de resultados auto evaluación	01/09/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla M8. Minuta de consulta con tutor.

Reunión No.	21	**Fecha:**	01/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	05:30 pm. /06:25 pm
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Revisión del avance en Marco Teórico	Se definen las secciones del marco teórico a ser desarrolladas.	Se realizan los comentarios sugeridos por parte del tutor. Responsable: Bryan Blanco
2	Auditoría de cumplimiento	Se comentan los acuerdos de la reunión con la profesora Laura Alpizar. Se realizan recomendaciones para la documentación de los resultados.	Se toman las notas y se aplican las recomendaciones. Responsable: Bryan Blanco
3	Revisiones del cronograma	Revisión del avance y entregas pendientes.	Se aprueba el avance por parte del tutor. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	**Fecha**	**Convocados**
Consulta de seguimiento	08/09/2021	Carlos Mata y Bryan Blanco

Tabla M9. Minuta de seguimiento con tutor.

Reunión No.	24	**Fecha:**	08/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	05:00 pm. /05:45 pm
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Revisión de análisis de brecha	Se establecen las brechas de acuerdo al estado actual.	Se aprueba el análisis por parte del tutor. Responsable: Carlos Mata
2	Revisión del análisis de clientes	Se aprueban las áreas incluidas como parte de la alineación del SGSI con los requerimientos de la empresa.	Se toman las notas y se aplican las recomendaciones. Responsable: Bryan Blanco
3	Revisiones del cronograma	Revisión del avance y entregas pendientes.	Se aprueba el avance por parte del tutor. Responsable: Bryan Blanco
4	Metodología	Se define la estructura de la metodología tomando como referencia el libro de metodología de la investigación de Hernandez Sampieri	Se enviará el libro por parte del profesor. Responsable: Carlos Mata

Próxima reunión		
Temas a tratar	**Fecha**	**Convocados**
Consulta de seguimiento	15/09/2021	Carlos Mata y Bryan Blanco

Tabla M10. Minuta de consulta de seguimiento.

Reunión No.	27	**Fecha:**	15/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	05:00 pm. /06:15 pm
Objetivo de la reunión:	Consulta de seguimiento		

Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Revisión de análisis de capacidad	Se aprueba el análisis de capacidad definido con la profesora Laura Alpizar.	Se aprueba el análisis por parte del tutor. Responsable: Carlos Mata
2	Revisión del avance en la metodología	Se establece el enfoque mixto. Se establecen las categorías de análisis. Se definen los instrumentos e indicadores para cada fase.	Se toman las notas y se aplican las recomendaciones. Responsable: Bryan Blanco
3	Revisiones del cronograma	Revisión del avance y entregas pendientes.	Se aprueba el avance por parte del tutor. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Consulta de seguimiento		24/09/2021	Carlos Mata y Bryan Blanco

Tabla M11. Minuta de consulta de seguimiento.

Reunión No.	32	**Fecha:**	24/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	10:00 am. /10:40 am
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Revisión de la estructura para análisis de resultados	Se definen las secciones del análisis de resultados a ser desarrolladas.	Se realizan los comentarios sugeridos por parte del tutor. Responsable: Bryan Blanco
2	Estado meta	Se comentan las necesidades para una certificación y se consultará a profesores afines a la materia. Dos principios básicos de certificación: Gestión basada	Se coordinará consulta con profesores de la carrera. Responsable: Bryan Blanco

		en riesgos y mejoramiento continuo.	
3	Niveles de capacidad	Determinar la brecha a través de los criterios definidos para el estado actual y los niveles de capacidad COBIT 2019.	Adoptar las recomendaciones y comentarios. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Consulta de estudio de mercado		24/09/2021	Carlos Mata y Bryan Blanco

Tabla M12. Minuta de estudio de mercado.

Reunión No.	33	**Fecha:**	24/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	5:30 pm. /06:00 pm
Objetivo de la reunión:	Consulta estudio de mercado		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Revisión de la estructura para estudio de mercado	Se definen los objetivos del estudio de mercado.	Se define la estructura sugerida por parte del tutor. Responsable: Bryan Blanco
2	Enfoque de la oferta y demanda	La oferta se enfoca en empresas certificadoras y la demanda en los usuarios (clientes y departamento de TI).	Revisar oferta de certificaciones e involucrados. Responsable: Bryan Blanco
3	Definir el producto	SGSI definido como producto industrial y su distribución.	Definir la estrategia. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Consulta de seguimiento		29/09/2021	Carlos Mata y Bryan Blanco

Tabla M13. Minuta de consulta de seguimiento.

Reunión No.	35	**Fecha:**	29/09/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	10:00 am. /10:40 am
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	**Revisión capítulo III**	**Se revisan las correcciones realizadas por el tutor.**	**Se aprueban los cambios realizados. Responsable: Bryan Blanco**
2	**Revisión capítulo IV**	**Se revisa el avance del capítulo y se generan las recomendaciones necesarias.**	**Se toman las recomendaciones para ser aplicadas. Responsable: Bryan Blanco**
3	**Revisión de cronograma**	**Se revisa el avance y se coordinan las actividades de la siguiente semana.**	**Continuar con las actividades acordadas. Responsable: Bryan Blanco**
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Seguimiento de avance		06/10/2021	Carlos Mata y Bryan Blanco

Tabla M14. Minuta de consulta de seguimiento.

Reunión No.	42	**Fecha:**	15/10/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	09:00 am. / 09:50 am
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**

1	Proceso de gestión de la seguridad de la información.	Se verifica el diagrama BPMN As-Is y To-Be del proceso por parte del tutor.	Documentar las observaciones de mejora. Responsable: Bryan Blanco.
2	Gestión de riesgos	Se verifica los criterios de identificación y evaluación de riesgos	Se aplican las recomendaciones. Responsable: Bryan Blanco
3	Clasificación y etiquetado de activos.	Se verifican los criterios y las fuentes de referencia para la clasificación y etiquetado de los activos de información.	Se aplican las recomendaciones. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Procesos BPMN		13/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla M15. Minuta de revisión y ajustes al documento final.

Reunión No.	47	**Fecha:**	27/10/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	05:00 pm. / 06:30 pm
Objetivo de la reunión:	Revisión y ajustes al documento final		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Ajuste en título del documento y objetivos del proyecto.	Se ajusta el título y objetivos para alinear al alcance del proyecto.	Se realizan los ajustes en el título del proyecto de acuerdo a recomendaciones. Se ajustan detalles en los objetivos para el alineamiento. Responsable: Bryan Blanco

2	Se evalúa el planteamiento del problema para verificar la propuesta	Se verifican el árbol de problemas y el árbol de objetivos.	Se documentan y aplican las recomendaciones brindadas por parte del tutor. Responsable: Bryan Blanco
3	Revisión del alcance	Se verifica que las tareas realizadas se encuentren acorde al alcance establecido.	Se establecen los objetivos del caso de negocio alineados con el alcance del proyecto. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
Reunión de seguimiento.		03/11/2021	Carlos Mata y Bryan Blanco

Tabla M16. Minuta de revisión y ajustes al documento final.

Reunión No.	47	**Fecha:**	03/11/2021
Lugar:	Microsoft Teams	**Hora Inicio/Finalización:**	06:00 pm. / 08:30 pm
Objetivo de la reunión:	Revisión y ajustes al documento final		
Participantes:	Presentes: Carlos Mata y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	Ajustes en caso de negocio	Se revisan y corrigen los estudios realizados	Se realizan los ajustes en el caso de negocio de acuerdo a recomendaciones. Responsable: Bryan Blanco
2	Plan de implementación.	Se revisa y se realizan recomendaciones en cronograma y plan de implementación.	Se aplican las recomendaciones. Responsable: Bryan Blanco

3	Conclusiones y recomendaciones	Se verifican las conclusiones y recomendaciones del proyecto.	Se aplican las recomendaciones. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados**
-		-	-

Apéndice N. Minutas de Reuniones con la Organización.

Tabla N1. Minuta de entrevista con analista de negocio de TI.

Reunión No.	01	Fecha:	26/06/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	9:30 am. / 10:30 am
Objetivo de la reunión:	Resultado de entrevista con analista de negocio de TI.		
Participantes:	Presentes: Paola Solano y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Consulta sobre los problemas presentados actualmente en la empresa	Los problemas se enfocan en la rigurosidad de los clientes, la necesidad de un panorama claro y una estandarización.	Alinear el problema del proyecto. Responsable: Bryan Blanco
2	Consulta por estructura establecida por la empresa para el desarrollo de caso de negocio	No se tiene un formato establecido.	Se analizarán las secciones del documento que sean necesarias para determinar la viabilidad con sus respectivos estudios y análisis. Responsable: Bryan Blanco
3	Consulta por recomendaciones generales	Evitar una extensión innecesaria del documento, tratar de ser lo más conciso posible	Se tomarán las recomendaciones y se aplicarán en el documento. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	Fecha	Convocados
Recomendaciones por parte de profesores y entrevista a Javier Araya	29/06/2021	Paola Solano, Javier Araya y Bryan Blanco.

Tabla N2. Minuta de entrevista con analista de negocio de CRM.

Reunión No.	02	Fecha:	29/06/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	11:00 am. / 11:40 am
Objetivo de la reunión:	Ajustes del documento y resultado de entrevista con analista de negocio de CRM.		
Participantes:	Presentes: Paola Solano, Javier Araya, Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Consulta sobre las recomendaciones de profesores y cambios en objetivos.	Si se busca una certificación se debe optar por ISO 27001. Para determinar la viabilidad se requieren datos financieros.	Alinear el documento a los nuevos objetivos. Los datos sensibles se trabajarán bajo acuerdos de confidencialidad. Responsable: Bryan Blanco
2	Breve entrevista a Javier Araya	Se reciben las respuestas detalladas y perspectiva del problema del CRM Business Analyst	Se documentan las respuestas y se aplicarán los ajustes en el documento. Responsable: Bryan Blanco
3	Resultado de respuestas	Se requiere una estandarización del proceso que facilite la verificación del cumplimiento de los requerimientos por parte de los clientes. Existen limitaciones en personal del departamento y podría presentarse resistencia al cambio por parte de colaboradores.	Se documentan las respuestas y se aplicarán los ajustes en el problema y alcance del proyecto. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	Fecha	Convocados
Primeras indicaciones por parte de la empresa. Correcciones y revisión del documento.	13/07/ 2021	Paola Solano, Javier Araya, Christian Campos y Bryan Blanco.

Tabla N3. Minuta de primeras indicaciones por parte de la empresa.

Reunión No.	05	Fecha:	13/07/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	9:30 am. / 10:30 am
Objetivo de la reunión:	Primeras indicaciones por parte de la empresa		
Participantes:	Presentes: Paola Solano, Javier Araya, Christian Campos, Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Consulta por los clientes de la empresa	Los clientes al ser de diferentes industrias requieren flexibilidad para adaptar los controles según sus requerimientos.	Anotaciones relevantes para el proyecto. Responsable: Bryan Blanco
2	Creación de Gantt	Necesario para el control del cronograma y avance del proyecto.	Crear el documento. Responsable: Bryan Blanco
3	Uso adecuado del Planner y calendario.	Agregar las tarjetas con sus tareas, responsable, prioridad y comentarios. Reservar las reuniones necesarias según la disponibilidad de los participantes.	Crear apartado con tareas. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	Fecha	Convocados
Situación actual de la empresa	15/07/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N4. Minuta de verificación de controles ISO 27001 actuales.

Reunión No.	06	Fecha:	29/07/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	10:00 am. / 10:30 am

Objetivo de la reunión:	Verificación de controles ISO 27001 actuales		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Verificación de áreas de controles ISO 27001 incluidas en la matriz	Registro y documentación de la situación actual en los diferentes controles así como las observaciones por parte de los analistas de negocio	Documentación de las observaciones en el documento “Verificación de controles ISO 27001”. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Continuar con la verificación de controles		29/07/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N5. Minuta de primera reunión entre tutor, estudiante y empresa.

Reunión No.	12	Fecha:	12/08/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	14:55 pm. / 15:55 pm
Objetivo de la reunión:	Primera reunión entre tutor, estudiante y empresa.		
Participantes:	Presentes: Paola Solano, Javier Araya, Carlos Mata, Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Presentación ejecutiva del proyecto	Se realizan comentarios en torno al fondo del proyecto.	Aplicar las decisiones acordadas por las partes. Responsable: Bryan Blanco
2	Dudas relacionadas al alcance	Se establece la visión desde la infraestructura de TI para el alcance del proyecto.	Realizar los cambios en el Capítulo I. Responsable: Bryan Blanco

3	Detalles del proyecto	Se brindan los documentos confidenciales necesarios para el proyecto. Se establecen los detalles del análisis de la industria y los elementos del caso de negocio.	Se reciben los documentos y se aplican los comentarios en el proyecto. Responsable: Bryan Blanco.
4	Operacionalización de variables del objetivo 1	Se establecen los atributos, la conceptualización, indicadores e instrumentos para el primer objetivo	Se tomarán las recomendaciones y se aplicarán en el documento. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados

Tabla N6. Revisión general del documento.

Reunión No.	16	Fecha:	20/08/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	1:00 pm. / 2:00 pm
Objetivo de la reunión:	Revisión de Capítulo I		
Participantes:	Presentes: Paola Solano y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Revisión del Capítulo I del TFG	Se realizan comentarios y observaciones por parte de la mentora Paola Solano.	Realizar los cambios y tomar las observaciones realizadas. Responsable: Bryan Blanco
2	Priorización de brechas	Se establece la necesidad de clientes e industria así como la capacidad de la empresa como criterios de priorización	Realizar las adaptaciones y tomar los acuerdos para ser aplicados. Responsable: Bryan Blanco

3	Estructura del caso de negocio	Cada una de las fases serán un insumo para el desarrollo del caso de negocio.	Realizar diagrama de la fase inicial. Aplicar los comentarios en la ejecución del proyecto. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Continuar con la revisión del documento		23/08/2021	Paola Solano y Bryan Blanco

Tabla N7. Minuta de identificación de indicadores clave de rendimiento con el equipo de trabajo.

Reunión No.	19	Fecha:	26/08/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	10:00 am. / 10:30 am
Objetivo de la reunión:	Definición de los KPI.		
Participantes:	Presentes: Paola Solano, Javier Araya, Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Analizar los objetivos del departamento	Se establecen los objetivos y kpis de los responsables que serán atendidos con el proyecto	Documentar los KPIs Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Siguientes pasos del proyecto		06/09/2021	Paola Solano, Javier Araya,y Bryan Blanco.

Tabla N8. Minuta de consulta a auditor experto.

Reunión No.	20	Fecha:	01/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	05:00 pm. /05:30 pm

Objetivo de la reunión:	Verificación de la propuesta de SGSI		
Participantes:	Presentes: Laura Alpizar y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Revisión del SGSI	Se realizan observaciones de forma en el documento. Se aprueban las acciones y avance. Recomendación de evaluación por área.	Se toman las observaciones y recomendaciones. Responsable: Bryan Blanco
2	Niveles de capacidad	Se comentan los acuerdos de la reunión con la profesora Laura Alpizar. Se realizan recomendaciones para la documentación de los resultados.	Tomar como referencia niveles de capacidad COBIT 2019 Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Consulta de seguimiento		01/09/2021	Carlos Mata y Bryan Blanco

Tabla N9. Minuta de revisión de avance con el equipo de trabajo.

Reunión No.	22	Fecha:	02/09/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	10:00 am. / 10:30 am
Objetivo de la reunión:	Revisión de avance		
Participantes:	Presentes: Paola Solano, Javier Araya, Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Avance del documento correspondiente al SGSI	Se verifican los últimos controles pendientes.	Se documentan las verificaciones realizadas. Responsable: Bryan Blanco

2	Marco teórico	Se define la estructura del caso de negocio.	Se toman las observaciones para definir el caso. Responsable: Bryan Blanco
3	Cronograma	Revisión y actualización de las tareas.	Se aprueban los cambios y avances. Responsable: Paola Solano
Próxima reunión			
Temas a tratar		Fecha	Convocados
Revisión de seguimiento		10/09/2021	Paola Solano, Javier Araya,y Bryan Blanco.

Tabla N10. Minuta para definir los siguientes pasos del proyecto.

Reunión No.	23	Fecha:	06/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	02:00 pm. /02:30 pm
Objetivo de la reunión:	Siguientes pasos		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Análisis de brecha	Se definen pesos para el Estado Actual de cada control de forma que sea el criterio de evaluación para determinar las brechas.	Se definen los pesos a cada estado actual. Responsable: Bryan Blanco
2	Análisis de requerimientos de clientes	Se definen las áreas y controles a incluir en el SGSI por parte de los requerimientos de los clientes.	Agregar las áreas y los controles definidos. Responsable: Bryan Blanco
3	Resultados	Se determina que los resultados se reflejan en la herramienta de Excel Evaluación de la seguridad de la información de forma holística.	Se identificarán en el documento los requerimientos de ISO 27001 y los requerimientos de clientes. Responsable: Bryan Blanco
Próxima reunión			

Temas a tratar	Fecha	Convocados
Revisión de documento TFG	17/09/2021	Paola Solano y Bryan Blanco

Tabla N11. Minuta de verificación de la matriz.

Reunión No.	25	Fecha:	10/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	10:00 am. /10:40 am
Objetivo de la reunión:	Verificación de avance		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Estructura del SGSI	Se define la forma para incluir los criterios de evaluación y la verificación de controles y análisis de brecha.	Se realizaron los cambios en el documento de Excel. Responsable: Bryan Blanco
2	Verificación de controles	Se realiza la última verificación de los controles correspondientes al análisis de clientes.	Se documentan las acciones en cada control. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	Fecha	Convocados
Seguimiento del proyecto.	16/09/2021	Paola Solano y Bryan Blanco

Tabla N12. Minuta de consulta con experto auditor.

Reunión No.	26	Fecha:	14/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	05:15 pm. /05:30 pm
Objetivo de la reunión:	Análisis de capacidad		
Participantes:	Presentes: Laura Alpizar y Bryan Blanco		
	Ausentes:		
Temas Tratados			

No.	Asunto	Comentarios	Acuerdos
1	Análisis de capacidad	Se recomienda por parte de la profesora utilizar los niveles de capacidad COBIT 2019 y los resultados de las brechas para definir los niveles de capacidad.	Se toman las recomendaciones de la profesora
Próxima reunión			
Temas a tratar		Fecha	Convocados
Consulta de seguimiento		01/09/2021	Carlos Mata y Bryan Blanco

Tabla N13. Minuta de seguimiento del proyecto.

Reunión No.	28	Fecha:	16/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	10:00 am. /10:30 am
Objetivo de la reunión:	Seguimiento del proyecto		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Verificación de controles	Se verifica la revisión documental y registro realizado en la política de privacidad.	Se realizaron los cambios en el documento de Excel. Responsable: Bryan Blanco
2	Estado meta	Se define como objetivo llevar los procesos hacia un estado de largamente.	Se toman las observaciones para aplicar como acuerdos. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Seguimiento del proyecto		23/09/2021	Paola Solano y Bryan Blanco

Tabla N14. Minuta de avance de proyecto.

Reunión No.	30	Fecha:	20/09/2021

Lugar:	Microsoft Teams	Hora Inicio/Finalización:	02:00 pm. / 02:45 pm
Objetivo de la reunión:	Avance de proyecto		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Operacionalización de variables.	Se establece la contextualización de las categorías de análisis. Se acota el segundo objetivo a las brechas.	Se toman y aplican las recomendaciones realizadas. Responsable: Bryan Blanco
2	Estudio de mercado	Se definen los aspectos a tomar en cuenta en el análisis.(Oferta, demanda, producto y distribución)	Se define estructura de análisis de mercado. Responsable: Bryan Blanco

Próxima reunión		
Temas a tratar	Fecha	Convocados
Seguimiento de avance	23/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N15. Minuta de estructura análisis técnico.

Reunión No.	31	Fecha:	23/09/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	02:00 pm. / 02:45 pm
Objetivo de la reunión:	Estructura análisis técnico		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Revisión de las secciones.	Se establece enfocar el tamaño en las brechas y la localización en la red.	Se toman y aplican las recomendaciones realizadas. Responsable: Bryan Blanco

2	Verificación del análisis de capacidad	Se revisan los resultados y se aprueban por parte de los encargados.	Establecer la priorización de brechas. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Revisión del documento TFG.		29/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N16. Minuta de revisión de avance y seguimiento con el Director de Seguridad.

Reunión No.	36	Fecha:	06/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	10:50 am. / 11:15 am
Objetivo de la reunión:	Revisión de avance y seguimiento		
Participantes:	Presentes: Juan José Mena y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Matriz Evaluación de Seguridad de la Información.	Se muestra la matriz de evaluación y se aprueba por parte del Director de seguridad.	Aprobación del avance. Responsable: Juan José Mena
2	Brechas y capacidad	Se muestran las brechas y niveles de capacidad para cada área de control y se aprueba por parte del Director de seguridad.	Aprobación del avance. Responsable: Juan José Mena
3	Estrategia de distribución	Se establecen los intereses y aportes de cada involucrado así como los canales de distribución y uso del SGSI.	Se registran los comentarios en el análisis de mercado. Responsable: Bryan Blanco.
Próxima reunión			
Temas a tratar		Fecha	Convocados
Análisis de mercado		06/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N17. Minuta de revisión análisis de mercado.

Reunión No.	37	Fecha:	06/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	03:30 pm. / 03:50 pm
Objetivo de la reunión:	Revisión de análisis de mercado		
Participantes:	Presentes: Javier Araya, Paola Solano y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Fuentes primarias y secundarias	Se muestran los involucrados y las fuentes identificadas y se aprueba por parte de los colaboradores.	Aprobación del avance. Responsable: Paola Solano
2	Cotizaciones	Se envía la primera información para solicitar las cotizaciones en las organizaciones certificadoras.	Documentar los datos y enviar las solicitudes. Responsable: Bryan Blanco.
3	Estrategia de distribución	Se verifica la estrategia y los canales de distribución establecidos con el Director de Seguridad.	Se registran los comentarios en el análisis de mercado. Responsable: Bryan Blanco.
Próxima reunión			
Temas a tratar		Fecha	Convocados
Segunda Reunión entre tutor, estudiante y empresa.		08/10/2021	Paola Solano, Javier Araya, Carlos Mata y Bryan Blanco

Tabla N18. Minuta de segunda reunión entre tutor, estudiante y empresa.

Reunión No.	38	Fecha:	08/10/2021
Lugar:	Microsoft teams	Hora Inicio/Finalización:	14:55 pm. / 15:30 pm

Objetivo de la reunión:	Segunda reunión entre tutor, estudiante y empresa.		
Participantes:	Presentes: Paola Solano, Javier Araya, Carlos Mata, Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Presentación ejecutiva del avance en el proyecto	Se aceptan y aprueban los resultados presentados	Confirmar el avance. Responsable: Bryan Blanco
2	Pasos a seguir en el caso de negocio.	Se establece la propuesta de solución enfocada en las brechas encontradas.	Se toman y se aplican los acuerdos establecidos. Responsable: Bryan Blanco
3	Brechas a ser atendidas.	Como primer paso se llevan los procesos a Largamente y presentar las propuestas para llegar a completamente.	Se aplican los comentarios en el proyecto. Responsable: Bryan Blanco.
Próxima reunión			
Temas a tratar		Fecha	Convocados
Tercer reunión con la empresa y tutor		05/11/2021	Paola Solano, Javier Araya, Carlos Mata y Bryan Blanco.

Tabla N19. Minuta de estudio técnico.

Reunión No.	40	Fecha:	11/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	03:30 pm. / 03:50 pm
Objetivo de la reunión:	Establecer el tamaño óptimo del caso		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos

1	Requerimientos de la organización.	Los requerimientos deben estar enfocados en las brechas identificadas.	Se definen los requerimientos para definir el tamaño del caso de negocio. Responsable: Paola Solano
2	Organización humana y jurídicas necesarios a tomar en cuenta.	Se identifican las necesidades en la organización humana y se establecen las leyes que aplican al proyecto para ser tomadas en cuenta.	Se toman las recomendaciones y comentarios para aplicarlos en el análisis técnico. Responsable: Bryan Blanco
3	Disponibilidad y costo de insumos	Se establecen los recursos necesarios en materia de recurso humano y tiempos de ejecución de las tareas.	Se toman las recomendaciones y comentarios para aplicarlos en el análisis técnico. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Procesos BPMN		13/10/2021	Paola Solano, Javier Araya y Bryan Blanco.

Tabla N20. Minuta de procesos As-Is y To-Be.

Reunión No.	41	Fecha:	13/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	04:00 pm. / 04:50 pm
Objetivo de la reunión:	Definir los procesos As-is y to be.		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Gestión de la seguridad de la información.	Se establece el diagrama BPMN As-Is y To-Be del proceso.	Se documentan los diagramas. Responsable: Bryan Blanco.

2	Gestión de riesgos	Se establece el diagrama BPMN To-Be del proceso.	Se documenta el diagrama. Responsable: Bryan Blanco
3	Clasificación y etiquetado de activos.	Se establecen los criterios para la clasificación y etiquetado de los activos de información.	Se documentan los criterios. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Procesos BPMN		13/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N21. Minuta de verificación con equipo de trabajo.

Reunión No.	43	Fecha:	15/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	09:00 am. / 09:50 am
Objetivo de la reunión:	Consulta de seguimiento		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Cronograma y avance	Se verifica el cronograma y se identifican algunas tareas retrasadas por cambios y solicitud de información financiera.	Se solicitará la información por parte de la analista de negocio de TI. Responsable: Paola Solano
2	Activos de información	Se identifican los activos de información con los colaboradores del departamento.	Se aplican las recomendaciones. Responsable: Bryan Blanco
3	Clasificación y etiquetado de activos.	Se verifican los criterios y las fuentes de referencia para la clasificación y etiquetado de los activos de información.	Se aplican las recomendaciones. Responsable: Bryan Blanco
Próxima reunión			

Temas a tratar	Fecha	Convocados
Beneficios financieros	19/10/2021	Paola Solano, Juan Jose Mena y Bryan Blanco

Tabla N22. Minuta de estudio financiero.

Reunión No.	44	Fecha:	19/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	04:00 pm. / 04:30 am
Objetivo de la reunión:	Estudio financiero		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Análisis Costo-Beneficio	Se establece utilizar supuestos basados en riesgos para calcular el beneficio esperado al mitigar el incidente más crítico que puede generar altas pérdidas económicas y que con la certificación se pueden evitar.	Se documentan y aplican los acuerdos. Responsable: Bryan Blanco
2	Costos asociados	Se definen los recursos humanos y el tiempo como los criterios para definir el costo del proyecto.	Se documentan y aplican los acuerdos. Responsable: Bryan Blanco
3	Principales beneficios	Se establecen los beneficios desde una perspectiva estratégica tomando en cuenta objetivos, KPI´s y problemas presentados en el Departamento de TI.	Se aplican las recomendaciones y se documentan los principales beneficios estratégicos. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Costos de actividades		20/10/2021	Paola Solano y Bryan Blanco

Tabla N23. Minuta de costos de las actividades.

Reunión No.	45	Fecha:	20/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	10:00 am. / 11:30 am
Objetivo de la reunión:	Determinar el costo de las actividades del proceso.		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Costo por hora laboral	Se establece un promedio del costo por hora laboral en el Departamento de TI a cargo de llevar a cabo las actividades del proceso	Se documentan y aplican los acuerdos. Responsable: Bryan Blanco
2	Costos asociados a las actividades	Se definen los recursos humanos y el tiempo necesarios para las actividades que permitan definir el costo del proyecto en cada una de sus fases de implementación.	Se documentan y aplican los tiempos y recursos. Responsable: Bryan Blanco
3	Principales beneficios	Se establecen los beneficios desde una perspectiva estratégica tomando en cuenta objetivos, KPI´s y problemas presentados en el Departamento de TI.	Se aplican las recomendaciones y se documentan los principales beneficios estratégicos. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Identificación y análisis de riesgos		21/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N24. Minuta de evaluación de riesgos.

Reunión No.	46	Fecha:	26/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	09:00 am. / 10:30 am

Objetivo de la reunión:	Identificación, evaluación y tratamiento de los riesgos		
Participantes:	Presentes: Paola Solano, Javier Araya y Bryan Blanco		
	Ausentes:		
Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Verificar los riesgos identificados	Se verifican los riesgos asociados a la seguridad de la información identificados con los colaboradores del Departamento de TI.	Se realizan los ajustes de acuerdo a recomendaciones. Responsable: Bryan Blanco
2	Evaluación de riesgos	Se define la probabilidad y el impacto para cada uno de los riesgos identificados.	Se documentan los resultados de la probabilidad de impacto de cada riesgo. Responsable: Bryan Blanco
3	Estrategia de tratamiento	Se establecen las estrategias para el tratamiento de cada riesgo.	Se documentan las estrategias y medidas para el tratamiento de los riesgos. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Reunión de seguimiento.		28/10/2021	Paola Solano, Javier Araya y Bryan Blanco

Tabla N25. Minuta de análisis costo-beneficio.

Reunión No.	48	Fecha:	28/10/2021
Lugar:	Microsoft Teams	Hora Inicio/Finalización:	09:00 am. / 10:30 am
Objetivo de la reunión:	Análisis costo-beneficio		
Participantes:	Presentes: Javier Araya, Paola Solano, Juan Jose Mena y Bryan Blanco		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Establecer el criterio para el análisis	Se determina generar dos escenarios para evaluar su posible impacto.	Documentar la estructura de los escenarios. Responsable: Bryan Blanco
2	Escenarios	Se basan los escenarios en el impacto percibido en caso que se materialice el riesgo más crítico y sus repercusiones económicas.	Se documentan los escenarios y se establecen los criterios para medir el impacto económico. Responsable: Bryan Blanco
3	Análisis y cálculos	Se realizan los cálculos y supuestos del impacto percibido por cada escenario y los recursos humanos afectados.	Se documentan los datos y se realizan los cálculos del análisis costo-beneficio. Responsable: Bryan Blanco
Próxima reunión			
Temas a tratar		Fecha	Convocados
Reunión de seguimiento.		03/11/2021	Javier Araya y Bryan Blanco

Apéndice O. Cartas de certificación de firmas

Figura O.1. Carta de certificación de minutas con la empresa.

Carta de certificación de las minutas

Yo Paola Solano Castro, que poseo el rol de "Analista de negocio de TI" en el departamento de TI de Mobilize.net, además de, fungir como "mentora auxiliar" dentro del proyecto llamado "Propuesta de viabilidad mediante un caso de negocio en el Departamento de Tecnologías de Información para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013 en la empresa Mobilize.NET" desarrollado por el estudiante Bryan Blanco Morales, doy fe que las reuniones y minutas realizadas durante el tiempo de ejecución de este son verídicas. Por esto certifico la validez de las minutas presentadas en el "Apéndice A" del presente documento.

Analista de negocio de TI y mentora auxiliar del proyecto
Paola Solano Castro

Figura O.2. Carta de certificación de minutas con el tutor.

Carta de certificación de las minutas

Yo Luis Carlos Mata Montero, que poseo el rol de "Tutor" dentro del proyecto llamado "Propuesta de viabilidad mediante un caso de negocio en el Departamento de Tecnologías de Información para la certificación en gestión de la seguridad de la información con la norma ISO 27001:2013 en la empresa Mobilize.NET" desarrollado por el estudiante Bryan Blanco Morales, doy fe que las reuniones y minutas realizadas durante el tiempo de ejecución de este son verídicas. Por esto certifico la validez de las minutas presentadas en el "Apéndice M" del presente documento.

CARLOS LUIS MATA MONTERO (FIRMA)
Firmado digitalmente por CARLOS LUIS MATA MONTERO (FIRMA)
Fecha: 2021.11.09 08:13:35 -06'00'

Tutor del proyecto Carlos Mata Montero