UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

PROPUESTA DE UN PLAN DE DIRECCIÓN DE UN PROYECTO PARA AUDITAR UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA LA FIRMA DE CONSULTORIA EEQA

MAIKOL FERNANDO HERNANDEZ SEGURA

PROYECTO FINAL DE GRADUACION PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR POR EL TITULO DE MASTER EN ADMINISTRACION DE PROYECTOS

SAN JOSE, COSTA RICA

SEPTIEMBRE 2018

UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

Este Proyecto Final de Graduación fue aprobado por la Universidad como
Requisito parcial para optar al grado de Máster en Administración de Proyectos

_____
Jorge Trejos
PROFESOR TUTOR

_____
Luis Diego Argüello Araya
LECTOR No.1

_____
Fausto Fernández Martínez
LECTOR No.2

_____
Maikol Fernando Hernández Segura
SUSTENTANTE

DEDICATORIA

Gracias a Dios por el don de la vida y la innumerable cantidad de bendiciones que me rodean.

Por orden de aparición:

A mi valiente mamá, que siempre me mantuvo a raya en relación con mis responsabilidades académicas y cuyo seguimiento persiste al día de hoy.

A mi padre que está en el cielo, que me acompañó y me patrocinó el día que matriculé mi primera materia del bachillerato universitario.

A mi hermana, sangre de mi sangre.

A mi esposa, mi compañera de viaje, quien me impulsa a crecer y evolucionar como ser humano.

AGRADECIMIENTOS

A cada profesor que entregó su aporte personal para dar sentido y calidad a este proyecto educativo que he seguido.

A todo el personal administrativo de la UCI, por su profesionalismo mostrado a lo largo del programa de estudio.

INDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

INDICE DE ACRÓNIMOS Y ABREVIACIONES

- ACL - Siglas en inglés para el Lenguaje de Comandos de Auditoria (Audit Command Language)
- CAB – Siglas en ingles del Consejo Asesor de Cambios (Change Advisory Board)
- CGR - Contraloría General de la República
- CINDE - Coalición Costarricense de Iniciativas de Desarrollo
- CISA - Siglas en inglés de la Certificación de Auditor de Sistemas de Información (Certified Information Systems Auditor)
- CISM - Siglas en inglés de la Certificación en Gestión de Seguridad de la Información (Certified Information Security Manager)
- CONASSIF - Consejo Nacional de Supervisión del Sistema Financiero
- CRISC - Siglas en inglés de la Certificación en Riesgos y Control de Sistemas de Información (Certified in Risk and Information Systems Control)
- EDT- Estructura de Desglose de Trabajo
- EEQA - Siglas correspondientes a la primera letra de los apellidos de los Socios de Firma de Consultoría que busca implementar la auditoría del SGSI como servicio (Esquivel, Echeverría, Quesada y Alvarado)
- ISACA - Siglas en inglés de la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association)
- ITIL - Siglas en inglés de la Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library)
- ISO – Siglas en inglés de la Organización Internacional de Normalización (International Organization for Standardization)
- KPMG - Siglas corresponden a la primera letra de los apellidos de los Socios Fundadores de firma de auditoría, consultoría y asesoramiento legal y fiscal (Klynveld, Peat, Marwic y Goerdeler)

- PFG - Proyecto Final de Graduación
- PMBOK - Siglas en inglés de la Guía de los Fundamentos para la Dirección de Proyectos (Project Management Book of Knowledge)
- PMI - Siglas en inglés del Instituto de Administración de Proyectos (Project Management Institute)
- PWC - Siglas corresponden a la primera letra de los apellidos de los Socios Fundadores de la firma de auditoría, consultoría, asesoramiento legal y fiscal (Price, Waterhouse y Cooper)
- PYME- Pequeña y mediana empresa
- RBS - Siglas en inglés de la Estructura de Desglose de los Riesgos (Risk Breakdown Structure)
- SGSI - Sistema de Gestión de Seguridad de la Información
- SUGEF - Superintendencia General de Entidades Financieras
- SUPEN - Superintendencia de Pensiones
- TAACs - Técnicas de Auditoría Asistidas por Computadora
- TI - Tecnologías de la Información

RESUMEN EJECUTIVO

La Firma de Consultoría EEQA se funda en Costa Rica en el año 2009 por iniciativa de un grupo de expertos en las áreas de contaduría pública y auditoría, con la finalidad de brindar servicios profesionales en los campos de auditoría financiera, servicios contables, control interno y recientemente asesorías de índole legal. Las prácticas de calidad implementadas por la firma le han permitido consolidar una respetable cartera de clientes; sin embargo, el carácter emprendedor de sus socios fundadores, ha consignado como parte del plan estratégico para el periodo 2015-2020, el apuntalar las operaciones de la consultora en el país y expandir sus servicios profesionales en el istmo centroamericano.

No obstante, el continuo autoanálisis efectuado a lo interno de la firma, ha determinado que el crecimiento se ve afectado por la ausencia de un plan para desarrollar consultorías relacionadas con la gestión de las tecnologías de información, provocando que no se concreten algunas oportunidades de negocio principalmente con entidades financieras; al respecto, cabe destacar que los indicadores aportados por la Coalición Costarricense de Iniciativas de Desarrollo (CINDE), han colocado al sector de alta tecnología como el de mayor crecimiento en el país durante los últimos años.

Por consiguiente, la Firma EEQA requiere formular una propuesta de trabajo que le posibilite el desarrollar consultorías relacionadas con la gestión de las tecnologías de información, enfocándose en la evaluación de la razonabilidad de los Sistemas de Gestión de la Seguridad de la Información implementados por sus clientes. De esta forma, se pretende ganar dinamismo y repercusión mediática, lo que contribuye a mejorar sus posibilidades para suscribir un acuerdo con alguna firma internacional de consultoría, como estrategia para optimizar sus servicios profesionales, acrecentar su reputación y generar nuevos negocios que repercutan positivamente en los niveles de ingreso y rentabilidad.

Al respecto, se estableció como objetivo general del presente Proyecto Final de Graduación, crear una propuesta de un plan de dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para que la Firma Consultora EEQA pueda implementarlo como parte de su cartera de servicios profesionales.

Asimismo, se definió una serie de objetivos específicos que permitieron materializar el logro del objetivo supracitado; estos fueron: Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional, elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma, desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información. Preparar un plan de gestión de la calidad para

identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio, realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la Firma EEQA, que participará en el proyecto, generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto. Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI, desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas y finalmente, elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.

En lo correspondiente a la metodología empleada, fueron diversas las fuentes de información consultadas para el desarrollo del presente trabajo, tanto en formato impreso como digital. Como fuentes primarias, se coordinó entrevistas con el personal humano que conforma a la Firma de Consultoría EEQA, entre ellos se consideró a socios de la firma, a la gerencia de auditoría y miembros del equipo de auditores. También se revisó documentación propiedad de la firma, como lo fueron las lecciones aprendidas de proyectos anteriores y herramientas para identificar y gestionar riesgos de TI. Sobre las fuentes secundarias, se consideró oportuno la utilización del material desarrollado por el PMI, las directrices en materia tecnológica dictadas por el estado costarricense, la norma ISO/IEC 27001, el marco de referencia COBIT 5 y la metodología ITIL para le gestión de servicios de TI. En lo que respecta a los métodos de investigación, se aplicaron las técnicas Analítico-Sintético y el Inductivo-Deductivo.

Con el desarrollo del proyecto se obtiene como principal conclusión la importancia de aplicar las buenas prácticas para la gestión de proyectos, independientemente de la dimensión y de la complejidad del mismo. En el caso específico de la Firma EEQA, lo correspondiente a la gestión de proyectos es apenas una metodología incipiente, por lo que se enfatiza en lo relevante de su reforzamiento en todos los niveles de la organización. Como aspecto positivo se indica que toda la documentación generada durante el ciclo de vida del proyecto, incluyendo las lecciones aprendidas, pasarán a formar parte de los activos empresariales de la consultora.

Por otra parte, la principal recomendación radica en la obtención de certificaciones relacionadas con la gestión de los recursos de tecnologías de información, para el equipo de profesionales que conforma la Firma EEQA, ya que las mismas posicionan a un proveedor de servicios como un agente debidamente capacitado, a la vez que generan reputación empresarial; asimismo, es primordial que se incorpore el uso de herramientas tecnológicas como parte del plan de auditoría que busca implementar la firma, con la finalidad de proporcionar mayor profundidad a sus revisiones, lo que sin duda repercute en valor agregado para sus clientes.

1. INTRODUCCION

1.1 Antecedentes

La trayectoria de la Firma de Consultoría EEQA es breve, nacida en 2009 por iniciativa de un grupo de profesionales con amplia experiencia en los campos de contaduría pública y auditoría, en la actualidad su cartera de servicios profesionales incluye auditorías financieras, servicios contables, certificaciones de ingreso, elaboración de planillas, control interno y recientemente asesorías de índole legal.

Por otra parte, los distintos entes reguladores existentes en Costa Rica como son los casos de la Contraloría General de la República (CGR) y la Superintendencia General de Entidades Financieras (SUGEF), entre otros, han emitido directrices en materia de tecnologías de información de acatamiento obligatorio para las entidades sujetas a su regulación, creando la necesidad de optimizar aspectos tales como el gobierno de seguridad de la información, la gestión de riesgos tecnológicos, la administración del programa de seguridad de la información y la gestión de incidentes. Evaluar los elementos supra citados es una tarea compleja y la Firma EEQA no cuenta con el conocimiento y las herramientas necesarias para asumir dicha labor profesional.

1.2 Problemática.

La consultora EEQA es considerada una firma menor dentro del mercado costarricense donde tienen presencia las 4 consultoras más importantes a nivel mundial: PWC, Ernst & Young, KPMG y Deloitte. Estas consultoras cuentan con

una robusta y diversificada plataforma de servicios y metodologías de trabajo implementadas exitosamente en el país.

A pesar de ello, la Firma EEQA ha logrado consolidar relaciones comerciales con un pequeño pero constante grupo de clientes; no obstante, su plan estratégico 2015-2020 consigna entre sus objetivos prioritarios el desarrollar su propio plan de auditoría que le permita asesorar a sus clientes en relación con el estado actual del “Sistema de Gestión de Seguridad de la Información” y con ello materializar oportunidades de negocio e incrementar los niveles de ingreso y rentabilidad.

La ausencia del plan supra citado acarrea una serie de dificultades para la Firma EEQA, lo que ha truncado sus posibilidades de crecimiento y el expandir sus servicios a otros países de la región centroamericana. Recientemente fue descartada por una entidad financiera interesada en auditar tanto sus estados financieros como su plataforma tecnológica muy orientada al ambiente web. Otro caso evidente de estancamiento lo constituye la imposibilidad de suscribir un acuerdo con alguna firma internacional, lo cual le permitiría optimizar sus servicios beneficiando con ello a sus clientes quienes podrán favorecerse de la experiencia, normas de control de calidad y de la transferencia tecnológica y profesional.

Mientras EEQA no incorpore nuevos servicios profesionales, logre ampliar su número de clientes y goce de mayor reputación en el país, no parece probable que a mediano plazo se materialice un acuerdo como el idealizado por los socios de la consultora. Asociarse con alguna firma internacional sería un paso clave hacia el crecimiento y consolidación de la Firma EEQA, lo que incluso podría llevarle a cruzar fronteras.

A través del presente PFG se pretende brindar soporte a la consultora EEQA en el logro de sus objetivos organizacionales, para lo cual se desarrollarán los procesos de iniciación y planificación de conformidad con las buenas prácticas para la gestión de proyectos.

1.3 Justificación del problema

Toma relevancia la protección de la información como recurso invaluable para el éxito y permanencia de las organizaciones, al constituirse como el insumo fundamental para la toma decisiones; al respecto, su seguridad debe abordarse efectivamente ante la continua presencia de riesgos y amenazas que diariamente atentan contra su la integridad, disponibilidad y confidencialidad, por lo que es necesario el implementar una estrategia de seguridad de la información que incluya políticas, estándares y procedimientos para establecer la dirección de las organizaciones y controlar sus actividades.

Una serie de hechos suscitados en el país han venido a evidenciar la adquisición de conciencia sobre la importancia de gestionar la seguridad de la información y de instaurar criterios para gestionar el riesgo de las tecnologías de información así como los procesos de gobierno de TI, entre ellos se pueden citar:

1.3.1 Acuerdo SUGEF 14-09

El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), mediante artículo 6, del acta de la sesión 773-2009 del 20 de febrero del 2009 aprobó el Acuerdo SUGEF 14-09 “Reglamento sobre la gestión de la tecnología de información”, que define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas SUGEF. Asesorar a entidades financieras que deben cumplir con la norma supra citada, motivó a la firma EEQA a desarrollar su plan de auditoría para aplicarlo comercialmente, máxime que otras superintendencias entre ellas la de Pensiones (SUPEN), mediante la publicación en La Gaceta del 17 de abril de 2017 del “Reglamento general de gestión de la tecnología de información”, también han girado lineamientos similares que periódicamente deben ser objeto de revisión.

1.3.2 Ley de Protección de Datos

Ley No.8968 de protección de la persona frente al tratamiento de sus datos personales, publicada en la Gaceta No.170 del 05 de setiembre de 2011, cuyo ámbito de aplicación corresponde a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, así como toda modalidad de uso posterior de estos datos. La responsabilidad de tratar cuidadosamente los datos se evidencia a través del articulo No.10 denominado “Seguridad de los Datos”, el cual dicta: “El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.”

1.3.3 Delitos Informáticos y Conexos

La Asamblea Legislativa aprobó el 7 de junio de 2012, la reforma de la Sección VIII, Delitos Informáticos y Conexos, del Titulo VII del Código Penal, Ley No.9048, donde se especifican las sanciones para quienes cometan delitos relacionados con la violación de correspondencia o comunicaciones, estafa informática, daño informático, espionaje, suplantación de identidad, instalación o propagación de programas maliciosos, suplantación de páginas electrónicas y difusión de información falsa, entre otras situaciones estrechamente relacionadas con las tecnologías de información y que se detallan en los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley N.º 4573, Código Penal, de 4 de mayo de 1970. Esta reforma se publicó en la Gaceta No.214 del 06 de noviembre de 2012.

Por consiguiente, el desarrollar un plan de trabajo que le permita a la Firma EEQA aprovechar las oportunidades que surgen en el país, con motivo de los cambios en el marco normativo por el creciente auge de las tecnologías de información, se traduce como una solución para establecer nuevas oportunidades de negocio e incrementar los niveles de ingreso y rentabilidad, generando con ello el crecimiento empresarial del que actualmente carece EEQA.

De igual manera, brindar asesoramiento objetivo y profesional a sus clientes sobre las condiciones actuales del “Sistema de Gestión de Seguridad de la Información”, tendrá como beneficio complementario el ganar dinamismo y repercusión mediática, lo que contribuye a mejorar sus posibilidades para postularse como socio comercial de consultoras internacionales.

1.4 Objetivo general

El objetivo general del proyecto es crear una propuesta de un plan de dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para que la Firma Consultora EEQA pueda implementarlo como parte de su cartera de servicios profesionales.

1.5 Objetivos específicos.

Los objetivos específicos de este proyecto son:

- Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional.

- Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.
- Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información.
- Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.
- Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la firma EEQA, que participará en el proyecto.
- Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.
- Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.
- Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas.
- Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.

2. MARCO TEORICO

2.1 Marco Institucional

2.1.1 Antecedentes de la Institución

En el año 2007 se inició el proceso de negociación para la conformación de una nueva firma de consultoría que identificó como mercado meta a las denominadas PYMES dentro del mercado costarricense. La inquietud proviene de un grupo de 4 profesionales en contaduría pública, quienes en promedio habían ejercido por más de 10 años en distintas multinacionales dedicadas al sector de la consultoría profesional; asimismo, se incorporó al grupo un quinto miembro proveniente de la Contraloría General de la República.

La viabilidad de crear la firma rápidamente encontró sustento en una serie de indicadores que reflejaron la realidad de Costa Rica como parte del grupo de países líderes en la región por la calidad de su sistema educativo, la expansión del idioma inglés como segunda lengua, la apertura de las telecomunicaciones y su sólida infraestructura de servicios públicos; asimismo, la privilegiada posición geográfica en el centro de América, en medio de los océanos Pacífico y Atlántico, propiciaron la inversión de capital extranjero respaldado por el clima de negocios que impera en la nación.

El sector de alta tecnología es el que evidencia mayor crecimiento en Costa Rica durante los últimos años, situación que viene a evidenciar aún más la razonabilidad del objetivo de la Firma EEQA de incursionar en las auditorías de tecnologías de información. Al respecto, el informe presentado en Agosto de 2014 por el Sr. Jorge Rossi, presidente de la Junta Directiva de la Coalición Costarricense de Iniciativas de Desarrollo (CINDE), fue parte de la documentación analizada por los socios de EEQA, mientras se daba forma al plan estratégico de la firma para el quinquenio 2015-2020.

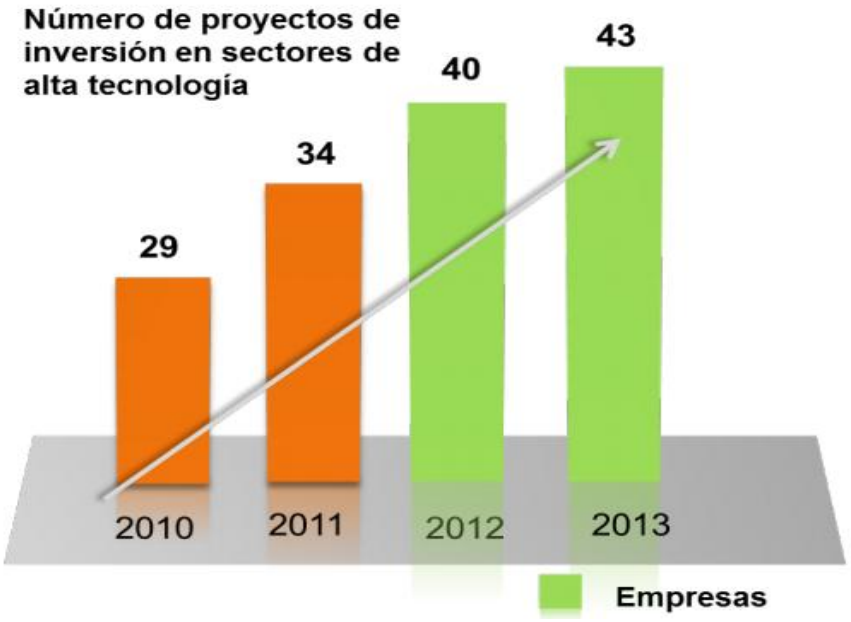


Gráfico No. 1. Proyectos de Inversión en Alta Tecnología
Fuente: (CINDE, 2014)

2.1.2 Misión y visión

Misión: "Ofrecer servicios profesionales con el objetivo de brindar soporte a nuestros clientes en el logro de sus metas organizacionales e incrementar la rentabilidad en sus operaciones." (Firma EEQA, 2015)

Visión: "Ser una firma de primer nivel en la prestación de servicios profesionales y consultoría, de conformidad con estándares de alta calidad y excelencia, que excedan las expectativas de nuestros clientes." (Firma EEQA, 2015)

2.1.3 Estructura organizativa

La estructura organizativa de EEQA corresponde a una estructura organizacional funcional, encabezada por el grupo de socios fundadores. Seguidamente, la Gerencia General se encarga de dirigir al resto de funcionarios que conforman la firma, entre los que destacan profesionales en los campos de contaduría pública,

derecho y administración de empresas. Cabe indicar que en la nómina no figura ningún ingeniero informático o similar.

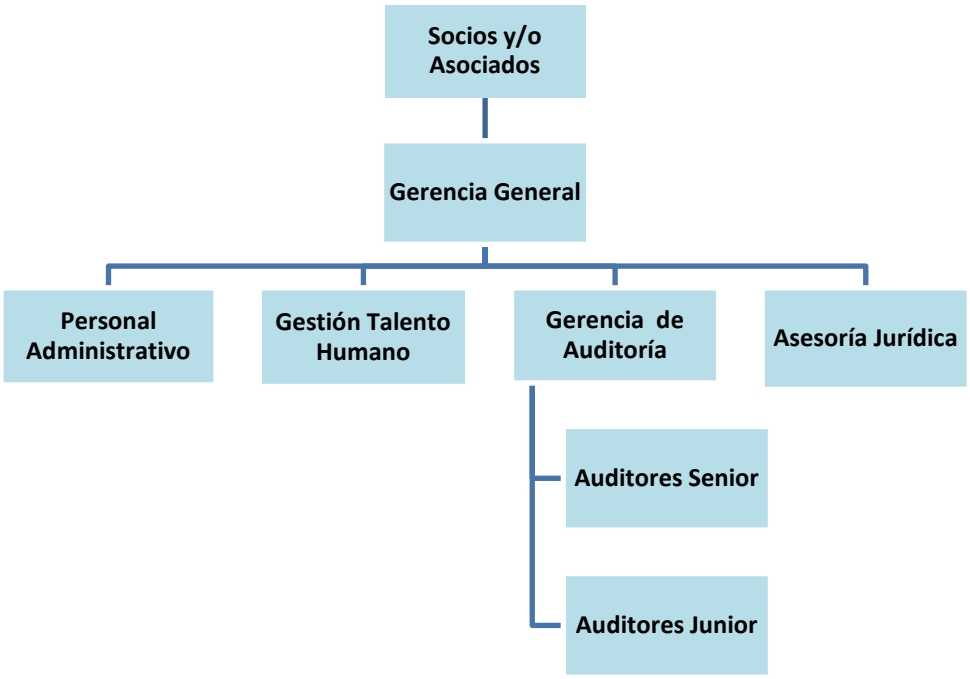


Figura No. 1. Estructura Organizativa – Firma EEQA
Fuente: (Firma EEQA, 2015)

2.1.4 Productos que ofrece

El principal servicio de la Firma EEQA corresponde a la planificación y ejecución de auditorías financieras, para lo cual anualmente se dirige aproximadamente el 70% de sus recursos; al respecto, el “Manual de normas generales de auditoría para el sector público”, emitido en 2006 por la CGR, consigna que la auditoría financiera: “comprende la auditoría de estados financieros que tiene por objetivo emitir un dictamen independiente sobre la razonabilidad de los estados financieros de la entidad auditada, de conformidad con el marco normativo aplicable” (p.3).

Como parte de la propuesta de servicio, EEQA desarrolla cada una de las fases sobre las cuales debe transcurrir el ejercicio de la auditoría, específicamente, la planeación y programación donde se delimita el alcance de la revisión para continuar con la ejecución del trabajo de campo para la recolección de evidencia que sustentará al informe final y al plan de acción para subsanar los hallazgos y las oportunidades de mejora identificadas; finalmente se efectuará el seguimiento a las recomendaciones emitidas. Entre los recursos a disposición de la firma, se encuentra la herramienta “Audit Command Language” (ACL), la cual permite leer y analizar diferentes tipos de archivos dispersos en numerosas bases de datos, lo que simplifica el proceso de revisión y clasificación de las transacciones.

La revisión del marco de control interno de las organizaciones, es otra de las principales actividades comerciales de la Firma EEQA, teniendo como objetivo la revisión de los planes, procedimientos, protección de los activos, confiabilidad de los registros contables y demás acciones ejecutadas por una entidad, con la finalidad de ofrecer seguridad razonable de que las operaciones se efectúan de conformidad con las normas y políticas establecidas por la administración, posibilitando con ello la conservación y protección del patrimonio organizacional y garantizar la eficiencia y eficacia de las operaciones. En el caso específico de Costa Rica, la Asamblea Legislativa promulgó la Ley General de Control Interno No.8292, la cual detalla los criterios mínimos de cumplimiento obligatorio para los entes u órganos sujetos a la fiscalización de la CGR.

El catálogo de servicios de la Firma EEQA se complementa con servicios de naturaleza contable, como lo son la preparación mensual de los estados financieros junto con sus respectivos anexos de gastos e ingresos, el registro de las operaciones en los libros de contabilidad correspondientes, conciliaciones bancarias y la emisión de documentos contables o reportes financieros requeridos por los clientes, entre ellos certificaciones de ingreso. También se ofrece el procesamiento de planillas acorde a la periodicidad que definan sus clientes, por lo es viable efectuar la preparación, cálculo y pago del salario, ya sea de forma

quincenal, semanal, mensual o cualquier otro diferente que la compañía tenga establecido. Adicionalmente, se efectúan el cálculo de aguinaldo, liquidaciones y el pago de las retenciones mensuales por concepto del impuesto sobre la renta. Finalmente, la EEQA suministra el servicio de tesorería para gestionar el pago a los proveedores, servicios públicos y demás compromisos de sus clientes.

2.2 Teoría de Administración de Proyectos

2.2.1 Proyecto

El Project Management Institute (2013) define que: “un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único” (p. 2). Por consiguiente, es fundamental que exista una metodología que posibilite guiar todos los recursos y equilibrar las restricciones contrapuestas para alcanzar los objetivos trazados.

2.2.2 Administración de Proyectos

La administración de proyectos a través de la aplicación de habilidades y conocimientos, el uso de herramientas y de las técnicas adecuadas, permite gestionar las actividades de un proyecto, completar los entregables y alcanzar los requerimientos definidos. La administración de proyectos involucra una serie buenas prácticas aplicadas de forma estructurada lo que da origen a la estandarización; al respecto, la Organización Internacional de Estándares (ISO), desarrolló el estándar ISO 21500, consignando una guía de directrices para la dirección y gestión de proyectos.

La relevancia de administrar proyectos ha venido en aumento, específicamente en el campo de las tecnologías de información, ISACA ha reconocido que existe un riesgo considerable asociado con la gestión de proyectos, en caso de no existir un

control óptimo del mismo se pueden generar una serie de resultados adversos, entre ellos la pérdida de oportunidades de negocio, la pérdida de una ventaja competitiva y el incumplimiento de leyes y regulaciones, entre otros aspectos.

Cada organización presenta sus características únicas; sin embargo, lo que da valor a una metodología de administración de proyectos es su flexibilidad de poder ser adoptada por cualquier compañía, independientemente de sus dimensiones. De esta forma, se tendrá acceso a una valiosa herramienta que le permita abordar sus diversas necesidades y atender las expectativas de las distintas partes interesadas. Cabe indicar dirigir un proyecto debe alinearse con los objetivos estratégicos de una organización por lo que debe establecerse planes para lograr un alcance determinado.

2.2.3 Ciclo de vida de un proyecto

Debido a que un proyecto corresponde a un esfuerzo temporal donde deben existir un principio y un final claramente definidos, la administración de proyectos establece fases secuenciales cada una con sus propios objetivos, entregables intermedios e hitos específicos, que posibilitan desgranar la complejidad que encierra un proyecto si se analiza únicamente desde una perspectiva general. Las fases funcionan además como puntos de control para detectar y corregir errores.

Durante la fase de inicio se determinan las expectativas y los requerimientos que dan origen al proyecto, durante esta fase los riesgos y la incertidumbre son mayores; asimismo, el realizar algún cambio impactará en menor medida los costos del proyecto. Un documento clave es esta fase lo representa el Acta de Constitución del Proyecto.

Posteriormente, el siguiente paso corresponde a la organización y preparación para definir los recursos necesarios para desarrollar el proyecto y determinar las

actividades para completar el proyecto, identificar los factores críticos de éxito con los que medirá la aceptación de los entregables.

La ejecución del trabajo es la fase donde se lleva a cabo las actividades previamente planificadas con la finalidad de completar cada uno de los entregables solicitados. Finalmente, cuando se habla de la fase de cierre del proyecto, donde los principales interesados aprueban o desaprueban el resultado final del proyecto y las lecciones aprendidas durante el desarrollo del proyecto deben ser documentadas.

La figura No.2 representa gráficamente el ciclo de vida de un proyecto, según el PMI (2013):

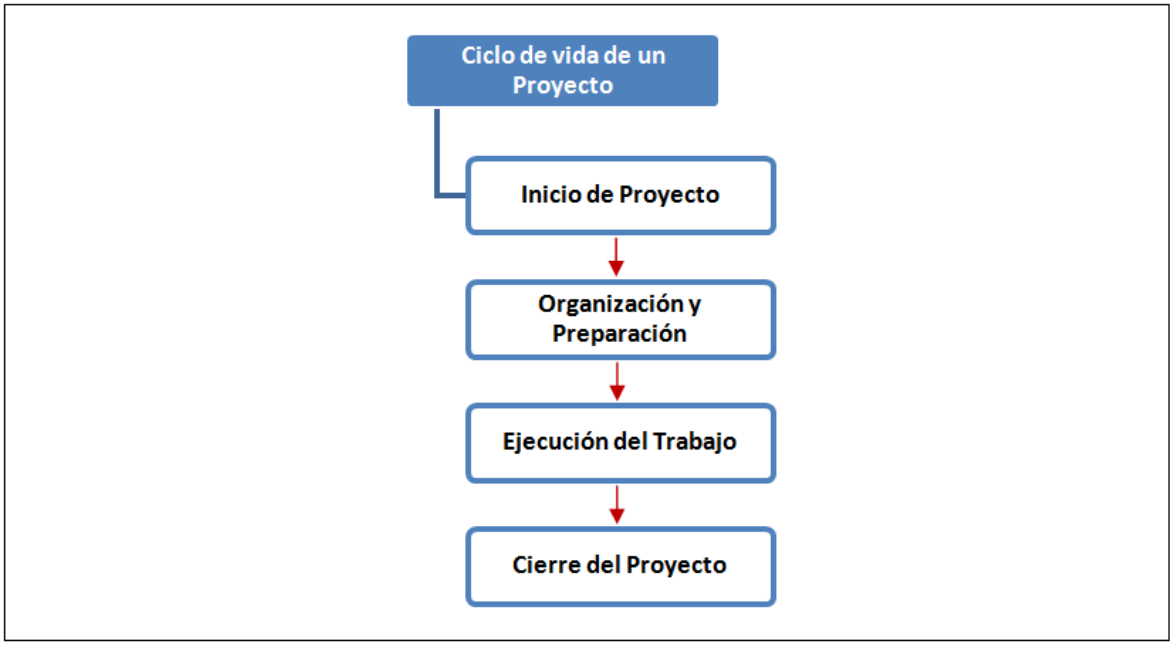


Figura No. 2. Ciclo de vida de un proyecto

Fuente: (PMI, 2013)

2.2.4 Procesos en la Administración de Proyectos

La quinta edición de la guía PMBOK (PMI, 2013), establece en 5 los grupos de procesos para la administración de proyectos los cuales “se utilizan para dirigir el

proyecto hacia un resultado más exitoso" (p, 17). De esta forma, es más sencillo el comprender y ejecutar un proyecto ya que el equipo de trabajo podría analizar los procesos adecuados y el nivel de detalle que se necesita para alcanzar los objetivos trazados, los cuales deben encontrarse integrados y alineados.

Los procesos se constituyen por entradas específicas de información, herramientas que pueden ser aplicadas para el desarrollo de cada uno de ellos y de esta forma generar salidas o entregables específicos de cada proceso. Los procesos además pueden ser utilizados como entradas para otros procesos.

En la figura No.3 se detallan los procesos en los que el PMI (2013) divide el ciclo de vida de un proyecto

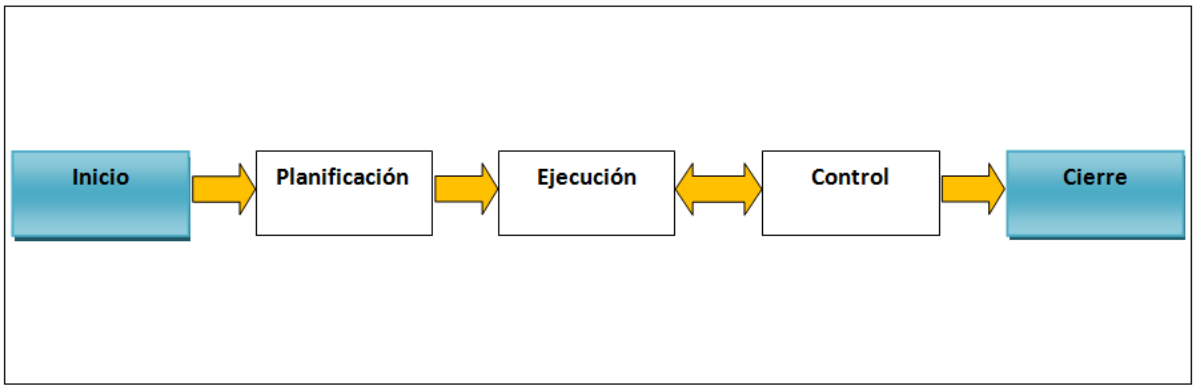


Figura No. 3. Procesos para la administración de proyectos
Fuente: (PMI, 2013)

- **Grupo de Procesos de Inicio:** Está compuesto por aquellos procesos realizados para definir un nuevo proyecto o una nueva fase de un proyecto existente al obtener la autorización para iniciar el proyecto o fase. Dentro del ámbito de los procesos de inicio es donde se define el alcance inicial y se comprometen los recursos financieros iniciales. Además, se identifican los interesados internos y externos que van a participar y ejercer alguna influencia sobre el resultado global del proyecto. Finalmente, si aún no hubiera sido nombrado, se selecciona el director del proyecto. Esta información se registra

en el acta de constitución del proyecto y en el registro de interesados. En el momento en que se aprueba el acta de constitución del proyecto, éste se considera oficialmente autorizado. (PMI, 2013, pág. 54).

- **Grupo de Procesos de Planificación:** Está compuesto por aquellos procesos realizados para establecer el alcance total del esfuerzo, definir y refinar los objetivos, y desarrollar la línea de acción requerida para alcanzar dichos objetivos. Los procesos de Planificación desarrollan el plan para la dirección del proyecto y los documentos del proyecto que se utilizarán para llevarlo a cabo. (PMI, 2013, pág. 55).

- **Grupo de Procesos de Ejecución:** Está compuesto por aquellos procesos realizados para completar el trabajo definido en el plan para la dirección del proyecto a fin de cumplir con las especificaciones del mismo. Este Grupo de Procesos implica coordinar personas y recursos, gestionar las expectativas de los interesados, así como integrar y realizar las actividades del proyecto conforme al plan para la dirección del proyecto. (PMI, 2013, pág. 56).

- **Grupo de Procesos de Monitoreo y Control:** Está compuesto por aquellos procesos requeridos para rastrear, analizar y dirigir el progreso y el desempeño del proyecto, para identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes. El beneficio clave de este Grupo de Procesos radica en que el desempeño del proyecto se mide y se analiza a intervalos regulares, y también como consecuencia de eventos adecuados o de determinadas condiciones de excepción, a fin de identificar variaciones respecto del plan para la dirección del proyecto. (PMI, 2013, pág. 57).

- **Grupo de Procesos de Cierre:** Está compuesto por aquellos procesos realizados para finalizar todas las actividades a través de todos los Grupos de Procesos de la Dirección de Proyectos, a fin de completar formalmente el proyecto, una fase del mismo u otras obligaciones contractuales. Este Grupo

> de Procesos, una vez completado, verifica que los procesos definidos se han completado dentro de todos los Grupos de Procesos a fin de cerrar el proyecto o una fase del mismo, según corresponda, y establece formalmente que el proyecto o fase del mismo ha finalizado. (PMI, 2013, pág. 57).

2.2.5 Áreas del Conocimiento de la Administración de Proyectos

Existen 47 procesos de la dirección de proyectos identificadas en la quinta edición de la Guía PMBOK (PMI, 2013), que *"se agrupan a su vez en diez Áreas de Conocimiento diferenciadas. Un Área de Conocimiento representa un conjunto completo de conceptos, términos y actividades que conforman un ámbito profesional, un ámbito de la dirección de proyectos o un área de especialización. Estas diez Áreas de Conocimiento se utilizan en la mayoría de los proyectos, durante la mayor parte del tiempo. Los equipos de proyecto deben utilizar estas diez Áreas de Conocimiento, así como otras áreas de conocimiento, de la manera más adecuada en su proyecto específico"*. (PMI, 2013, pág. 60).

Las Áreas de Conocimiento son: Gestión de la Integración del Proyecto, Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto, Gestión de los Costos del Proyecto, Gestión de la Calidad del Proyecto, Gestión de los Recursos Humanos del Proyecto, Gestión de las Comunicaciones del Proyecto, Gestión de los Riesgos del Proyecto, Gestión de las Adquisiciones del Proyecto y Gestión de los Interesados del Proyecto.

A continuación, se ilustrarán en el siguiente cuadro la integración de las diferentes áreas de conocimiento, los grupos de procesos y cada uno de los 47 procesos en un proyecto:

Cuadro No.1. Correspondencia entre los Grupos de Procesos y Áreas de Conocimiento y de la Dirección de Proyectos.

Áreas de Conocimiento	Grupos de Procesos de la Dirección de Proyectos				
	Grupo de Procesos de Inicio	**Grupo de Procesos de Planificación**	**Grupo de Procesos de Ejecución**	**Grupo de Procesos de Monitoreo y Control**	**Grupo de Procesos de Cierre**
Gestión de Integración del Proyecto	Desarrollar el Acta de Constitución del Proyecto.	Desarrollar el Plan para la Dirección del Proyecto.	Dirigir y Gestionar el Trabajo del Proyecto.	Monitorear y Controlar el Trabajo del Proyecto. Realizar el Control Integrado de Cambios.	Cerrar Proyecto o Fase.
Gestión del Alcance del Proyecto		Planificar la Gestión del Alcance. Recopilar Requisitos. Definir el Alcance. Crear la EDT/WBS.		Validar el Alcance. Controlar el Alcance.	
Gestión del Tiempo del Proyecto		Planificar la Gestión del Cronograma. Definir las Actividades. Secuenciar las Actividades. Estimar los Recursos de las Actividades. Estimar la Duración de las Actividades. Desarrollar el Cronograma.		Controlar el Cronograma	
Gestión de los Costos del Proyecto		Planificar la Gestión de los Costos. Estimar los Costos. Determinar el Presupuesto.		Controlar los Costos.	
Gestión de la Calidad del Proyecto		Planificar la Gestión de la Calidad.	Realizar el Aseguramiento de Calidad.	Controlar la Calidad.	
Gestión de los Recursos Humanos del Proyecto		Planificar la Gestión de los Recursos Humanos.	Adquirir el Equipo del Proyecto. Desarrollar el Equipo del Proyecto. Dirigir el Equipo del Proyecto.		
Gestión de las Comunicaciones del Proyecto		Planificar la Gestión de las Comunicaciones.		Controlar las Comunicaciones.	
Gestión de los Riesgos del Proyecto		Planificar la Gestión de los Riesgos. Identificar los Riesgos.		Controlar los Riesgos.	
Gestión de las Adquisiciones del Proyecto		Planificar la Gestión de las Adquisiciones.	Efectuar las Adquisiciones.	Controlar las Adquisiciones.	Cerrar las Adquisiciones.
Gestión de los Interesados del Proyecto	Identificar a los Interesados.	Planificar la Gestión de los Interesados.	Gestionar la Participación de los Interesados.	Controlar la Participación de los Interesados.	

Fuente: (PMI, 2013)

A continuación, se detallará cada una de las áreas de conocimiento consignadas en la quinta edición de la Guía PMBOK (PMI, 2013), las cuales sirven de soporte para el desarrollo del presente PFG:

2.2.5.1 Gestión de la Integración del Proyecto:

Incluye los procesos y actividades necesarios para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de dirección del proyecto dentro de los grupos de Procesos de Dirección de Proyectos (PMI, 2013, pág. 63). Permite que el proyecto contenga el trabajo requerido para que el mismo sea exitoso, para lo cual es esencial la toma de decisiones para asignar recursos y alternativas. Dentro de esta área de conocimiento se llevan a cabo los siguientes procesos:

- **Desarrollar el Acta de Proyecto:** Este documento autoriza formalmente la existencia del proyecto, otorgándole autoridad al director del proyecto en lo correspondiente a la asignación los recursos de la organización para el desarrollar el proyecto.
- **Desarrollar el Plan para la Dirección del Proyecto:** Determina todos los planes secundarios en un solo documento integral que posibilita la dirección del proyecto.
- **Dirigir y Gestionar el Trabajo del Proyecto:** Corresponde al proceso de liderar y ejecutar el trabajo planificado para implementar el proyecto.
- **Monitorear y Controlar el Trabajo del Proyecto:** Brinda seguimiento, revisa e informa sobre el avance de las actividades planeadas acorde con los objetivos dentro de los parámetros establecidos.
- **Realizar el Control de Cambios:** Proceso de evaluar y gestionar según corresponda, todas las solicitudes de cambio, así como efectuar la comunicación de las decisiones tomadas.

- **Cerrar el Proyecto o Fase:** Hace referencia a la finalización de todas las actividades para completar formalmente el proyecto en su totalidad o alguna de sus fases.

2.2.5.2 Gestión del Alcance del Proyecto:

Involucra los procesos que garantizan que el proyecto contenga todo el trabajo requerido para que el mismo sea exitoso. Gestionar el alcance del proyecto se enfoca fundamentalmente en definir y controlar los elementos que deben ser incluidos y que cuales deben ser descartados. Estos procesos son los siguientes:

- **Planificar la Gestión del Alcance:** Corresponde al proceso de formular el alcance del proyecto, formalmente documentado y que especifique la forma en que será definido, validado y controlado.
- **Recolección de Requisitos:** Determina, documenta y gestiona las necesidades y los requerimientos de los involucrados en el proyecto, para alcanzar los objetivos establecidos.
- **Definir el Alcance:** Corresponde al proceso de formular la descripción del alcance del proyecto.
- **Crear la EDT/WBS:** Consiste en separar los entregables del proyecto necesarios, de forma tal que completar cada uno de ellos sea menos complejo.
- **Validar Alcance:** Formaliza la aceptación de los entregables del proyecto que hayan sido completados de forma satisfactoria.
- **Controlar el Alcance:** Hace referencia al monitoreo y el control el avance del proyecto, así como de los productos o servicios versus las líneas base establecidas.

2.2.5.3 Gestión del Tiempo del Proyecto:

Contiene los procesos necesarios para finalizar el proyecto en el tiempo planificado, para lo cual se debe tener certeza sobre la inclusión de todas actividades, determinar su duración y secuenciarlas de forma razonable, lo contribuirá en la optimización de los tiempos de implementación. La gestión del tiempo del proyecto se conforma de los siguientes procesos:

- **Planificar la Gestión del Cronograma:** Se establecen las políticas, procedimientos y la documentación para la planeación, el desarrollo, la ejecución y el control del cronograma.
- **Definición de Actividades:** Contribuye en la identificación de las actividades necesarias para producir los entregables del proyecto, así como en su documentación.
- **Secuenciar Actividades:** Proceso mediante el cual se definen las relaciones entre las actividades del proyecto e integrarlas en una secuencia lógica.
- **Estimar Recursos para las Actividades:** Se estiman el tipo y cantidades de recursos, tanto materiales como humano, necesarios para realizar las actividades planificadas acorde con el alcance del proyecto.
- **Estimar Duraciones de Actividades:** Consiste en la estimación de la duración de los periodos de trabajo requeridos para llevar a cabo cada una de las actividades con los recursos estimados.
- **Desarrollar el Cronograma:** Proceso donde se analizan las secuencias de las actividades, su duración, los recursos requeridos y las restricciones de tiempos para desarrollar el Cronograma según lo planificado.
- **Controlar el Cronograma:** Considera los procesos de monitoreo y control de avance que presenta las actividades con respecto a las líneas base de tiempo, lo que permitirá determinar si se requiere concebir acciones adicionales y gestionar cambios para completar el proyecto exitosamente.

2.2.5.4 Gestión de los costos del Proyecto:

Reúne aquellos procesos vinculados con la planificación, la estimación, el presupuesto, el financiamiento y las actividades de monitoreo y control de los costos del requeridos por el proyecto, para que pueda ser finalizado de conformidad con el presupuesto que fue debidamente aprobado.
Los procesos que se contemplan son los siguientes:

- **Planificar la Gestión de los Costos:** Se determinan las políticas, procedimientos y la documentación requerida para el planeamiento, gestión, ejecución de recursos y control de los costos del proyecto.
- **Estimar los Costos:** Se establecen aproximaciones de recursos financieros para completar las actividades planificadas del proyecto.
- **Determinar el Presupuesto:** En este proceso se establecen las líneas base de costos, para lo cual es necesario totalizar los costos de cada paquete de trabajo así como de las actividades individuales.
- **Controlar los Costos:** Se refiere al proceso de monitorear y controlar los costos en los que se incurre en el proyecto para completar todas actividades y de actualizar los costos que se generen en caso de modificaciones en la línea base de costo.

2.2.5.5 Gestión de la Calidad del Proyecto:

El área de conocimiento incluye todos los procesos y actividades de la organización que determina las políticas, objetivos y responsabilidades para asegurar la calidad de los entregables que conforman el proyecto y apoyar las actividades de mejora continua. Para ello, es fundamental que los parámetros de calidad se encuentren definidos y se validen oportunamente. Los procesos que incluye esta área de conocimiento son los siguientes:

- **Planificar la Gestión de la Calidad:** Implica los procesos de identificación de los requisitos y estándares de calidad del proyecto establecido para cada entregable, conjuntamente con la documentación que evidencia el cumplimiento de las métricas de calidad aprobadas.
- **Realizar el Aseguramiento de Calidad:** La auditoría debe constituirse como un proceso objetivo, permanente y oportuno, que incluya los requerimientos y las normas de calidad.
- **Controlar de la Calidad:** A través de este proceso se monitorea y se registran los resultados obtenidos al efectuar la revisión de control de calidad, lo que permite a su vez la evaluación del desempeño del trabajo efectuado y suministrar recomendaciones que aporten valor.

2.2.5.6 Gestión del Recurso Humano del Proyecto:

En esta área de conocimiento se incorporan los procesos para organizar, gestionar y dirigir al equipo humano del proyecto. Al respecto, se debe tener en consideración las habilidades y conocimientos que se requieren para desarrollar las actividades que componen el proyecto, lo que permitirá la asignación de roles y responsabilidades al personal de acuerdo a sus características y competencias. El tiempo de asignación para cada recurso puede variar de completo a parcial o viceversa, acorde a las necesidades del proyecto; asimismo, otra buena práctica en relación a la gestión del recurso humano radica en fomentar la participación de todos los miembros del equipo en el proceso de toma de decisiones, lo cual fortalece la cohesión y el compromiso grupal.

Entre los procesos que comprenden esta área están:

- **Planificar la Gestión de los Recursos Humanos:** Corresponde a los procesos que identifican y documentan los roles, responsabilidades y habilidades necesarias, para formular un plan para la gestión de personal.

- **Adquirir el Equipo de Proyecto:** Referente a los procesos que reclutan a los miembros del equipo del proyecto. Verifican las condiciones de disponibilidad y los elementos necesarios para incorporar el equipo necesario para ejecutar las actividades del proyecto.
- **Desarrollar el Equipo del Proyecto:** Involucra a los procesos que contribuyen al mejoramiento de las competencias, las interacciones y el ambiente general que cubre al equipo de proyecto, con el objeto de optimizar los resultados obtenidos.
- **Dirigir el Equipo de Proyecto:** Se refiere al seguimiento sobre el desempeño del recurso humano con el objeto de brindar retroalimentación adecuada y oportuna a cada situación, solucionar problemas y gestionar los cambios que posibiliten optimizar el desenvolvimiento del equipo de proyecto.

2.2.5.7 Gestión de las Comunicaciones del Proyecto:

Involucra los procesos necesarios para asegurar la comunicación óptima entre las partes interesadas del proyecto, para lo cual es indispensable planificar la gestión de la información para lo cual se debe prestar atención en lo referente a su recolección, creación, distribución, almacenaje, manejo, monitoreo y control, tal y como lo apunta PMI (2013). La comunicación debe transitar oportunamente; no obstante, también debe considerarse en perspectiva los niveles de confidencialidad y protección que debe asignarse a la información. Los procesos que se desarrollan en ésta área de conocimiento son los siguientes:

- **Planificar la Gestión de las Comunicaciones:** Hace referencia al desarrollo del plan de comunicaciones del proyecto de conformidad con las necesidades y requisitos de las partes involucradas, en lo que respecta principalmente a la gestión de la información.

- **Gestionar las Comunicaciones:** Se crea, recopila, distribuye, almacena y se recupera según corresponda, la información del proyecto de acuerdo al plan de gestión de comunicaciones.
- **Controlar de las Comunicaciones:** Concierne a los procesos de monitoreo y control de la información, como medios para el aseguramiento de su valor y relevancia para satisfacer las necesidades informativas de los interesados del proyecto, durante todo el ciclo de vida del mismo.

2.2.5.8 Gestión del Riesgo del Proyecto:

Aquí residen los procesos para planificar la gestión de riesgos del proyecto, así como para efectuar la identificación, análisis, planificación de la respuesta y el control de los riesgos de un proyecto. De esta forma se pretende maximizar la probabilidad y el impacto de los eventos positivos, a la vez que se disminuye la probabilidad y el impacto de los eventos perjudiciales para el proyecto, lo cual representa el objetivo principal del área de conocimiento.

Los procesos que se desarrollan en esta área de conocimiento son los siguientes:

- **Planificar la Gestión de los Riesgos:** Hace referencia al proceso para definir el modo en que se gestionarán los riesgos inherentes de un proyecto.
- **Identificar del Riesgo:** Se determinan los riesgos que puedan afectar al proyecto y se documentan las características de cada uno de ellos.
- **Realizar el Análisis Cualitativo de Riesgos:** Consiste en la priorización de los riesgos identificados a través de la aplicación de los criterios de probabilidad de ocurrencia e impacto.
- **Realizar el Análisis Cuantitativo de Riesgos:** Se analiza desde una perspectiva numérica, los efectos de los riesgos en relación con el cumplimiento de los objetivos del proyecto.

- **Planificar la Respuesta a los Riesgos:** El establecimiento de planes de acción para mitigar los efectos de los riesgos identificados con la finalidad de materializar oportunidades de mejora y reducir las amenazas al proyecto.
- **Controlar los Riesgos:** Consiste en la implementación de los planes de respuesta al riesgo, lo que implica efectuar el seguimiento a los riesgos identificados una vez que los mismos son atendidos (riesgo residual) y evaluar la efectividad del plan de acción. De igual forma, analiza la prescencia de nuevos riesgos que puedan impactar al proyecto.

2.2.5.9 Gestión de las Adquisiciones del Proyecto:

Área de conocimiento que concentra los procesos necesarios para la adquisición de bienes o servicios, que deben obtenerse fuera del ámbito del equipo de proyecto. Con esto, las organizaciones pueden mantener de forma ordenada todos los cambios o inconvenientes que sucedan durante el proceso de adquisiciones.

Todas las organizaciones, independientemente si se tratan de compradoras o vendedoras de productos o servicios, deben gestionar sus contratos eficientemente. En consecuencia, se consideran aspectos tales como la gestión del contrato, el control de cambios y las órdenes de compra emitidas por miembros autorizados del equipo del proyecto, entre otros aspectos.

Entre los procesos que comprenden esta área están:

- **Planificar la Gestión de las Adquisiciones:** Se refiere al proceso de documentar las decisiones de adquisiciones necesarias para el proyecto y de la especificación del enfoque para identificar los probables proveedores del recurso.
- **Efectuar las Adquisiciones:** Inicia el proceso comunicación con el proveedor para determinar la viabilidad de la adquisición; posteriormente, se efectúa la selección y se determina la adjudicación del contrato.

- **Controlar las Adquisiciones:** Abarca la gestión de las relaciones de adquisiciones con los proveedores, así como el monitoreo de su desempeño para identificar puntos de mejora, efectuar cambios y correcciones en caso de ser necesarios.
- **Cerrar las Adquisiciones:** Corresponde a la finalización de cada uno de los procesos de adquisición de productos y servicios que se desarrollaron como parte de la implementación del proyecto.

2.2.5.10 Gestión de los Interesados del Proyecto:

Contiene los procesos para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, ya sea de forma positiva o negativa. Por lo tanto, se deben analizar las expectativas de los interesados y determinar su impacto en el proyecto, como medio para desarrollar estrategias de gestión adecuadas con el objetivo de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto.

La dirección del proyecto debe identificar correctamente a los sectores interesados del proyecto y optimizar las canales de comunicación para comprender sus necesidades y expectativas, gestionando los conflictos de intereses y fomentando una adecuada participación en la toma de decisiones y demás actividades del proyecto. Los principales procesos de esta área son:

- **Identificar a los Involucrados:** Se identifican a las personas, grupos u organizaciones que eventualmente podrían afectar o verse afectados por las decisiones tomadas y los resultados del proyecto. Sus intereses, participación, dependencias, influencia e impacto potencial sobre el proyecto, deben ser objeto de análisis.
- **Planificar la Gestión de los Interesados:** Formulación de estrategias de gestión convenientes para la eficaz participación de los interesados a lo largo

del ciclo de vida del proyecto, tomando en consideración las necesidades, intereses y el impacto en el éxito del proyecto.

- **Gestión la Participación de los Interesados:** Fomenta la oportuna participación de los interesados en las actividades del proyecto a lo largo de su ciclo de vida, haciendo uso de la comunicación y el trabajo con los interesados, como estrategia para satisfacer sus necesidades, expectativas y gestión oportuna de incidentes del proyecto.
- **Controlar la Participación de los Interesados:** Se monitorean las relaciones generales de los involucrados, ajustando las estrategias en caso de ser necesario para cumplir con las expectativas pactadas.

2.3 Seguridad de la Información

La norma ISO 27001 define la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad, así como de los sistemas implicados para su tratamiento, dentro de una organización (2013). Los términos anteriores, componen la base que soporta la seguridad de la información. Se entiende por información al conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o se transmita, de su origen o de su fecha de elaboración (ISO 27001, 2013).

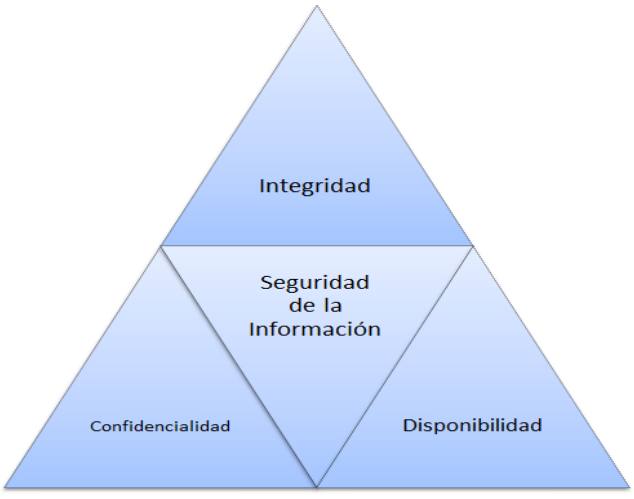


Figura No. 4. Seguridad de la Información

Fuente: (ISO 27001, 2013)

Por “Confidencialidad” se entiende que la información no debe ser revelada ni puesta a disposición de entidades, individuos o procesos que no se encuentran formalmente autorizados. Por su parte, la “Integridad” hace referencia al mantenimiento de la exactitud y completitud de la información y de sus métodos de procesamiento. En lo que respecta a la “Disponibilidad”, la información debe ser manejada por las entidades, individuos o procesos formalmente autorizados, en el momento que así lo requieran.

La seguridad de la información debe realizarse mediante un proceso sistemático, documentado y que sea de conocimiento por todos los miembros de una organización. Lo anterior, justifica la creación del Sistema de Gestión de Seguridad de la Información (SGSI), como instrumento para lograrlo.

Un SGSI comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos para implantar la gestión de la seguridad de la información. Para gestionar la seguridad de la información se debe considerar un conjunto de tareas y procedimientos que permitan garantizar los niveles de seguridad que son exigibles dentro de una organización, teniendo en consideración que los riesgos no se pueden eliminar en su totalidad; no obstante, pueden ser gestionados.

Al implementar un SGSI, una organización debe contemplar aspectos tales como la formalización de la gestión de la seguridad de la información, para lo cual se requiere el compromiso de la alta dirección, principalmente en lo referente a su establecimiento, revisión, mantenimiento y mejora; asimismo, los riesgos vinculados con la gestión de TI deben ser analizados y tratados oportunamente. En todo proceso en necesario visualizar un modelo que tenga en cuenta elementos tecnológicos, organizativos, el cumplimiento del marco legal y la relevancia del recurso humano.

El nivel de seguridad alcanzado por medios técnicos es insuficiente por sí mismo, por lo que la gestión efectiva de la seguridad debe tomar parte activa de toda la organización, lo cual incluye a su vez a los clientes y a los proveedores. El SGSI colabora en el establecimiento las políticas y procedimientos en relación con los objetivos del negocio de la organización, con la finalidad de mantener un nivel de exposición menor al nivel de riesgo que la propia organización ha admitido, para lo cual los riesgos pueden ser asumidos, minimizados, transferidos o controlados.

Es primordial que la alta gerencia tenga conocimiento del costo y el impacto de los incidentes de seguridad en términos económicos y de reputación para sus organizaciones. Algunas consecuencias de las posibles brechas de seguridad se manifiestan con las horas invertidas en las reparaciones y reconfiguración de la infraestructura tecnológica, pérdidas ocasionadas por la indisponibilidad de aplicaciones y servicios informáticos, robo de información confidencial, retrasos en los procesos de producción y pagos de indemnizaciones.

Para implementar un Sistema de Gestión de la Seguridad de la Información, una organización debe contemplar el denominado ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad:

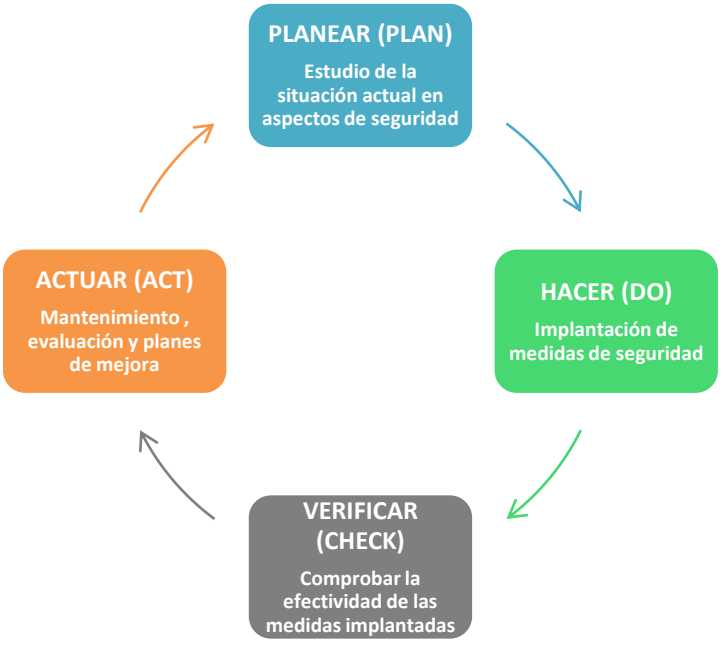


Figura No. 5. Metodología PDCA

Fuente: (ISO 27001, 2013)

La definición del alcance del SGSI debe incluir los términos del negocio, la organización, los activos y las tecnologías; asimismo, conlleva el establecimiento de una política de seguridad que establezca los objetivos de seguridad de la información y requerimientos legales. De igual forma, se debe definir una metodología de evaluación de riesgos que consigne los criterios de aceptación del mismo y de evaluación de los niveles de probabilidad e impacto.

Finalmente, los roles y las responsabilidades deben encontrarse claramente definidos y haber sido formalmente comunicadas, para lo cual se debe tener en consideración buenas prácticas de seguridad como lo es la segregación de funciones. Se deben determinar las competencias necesarias para que el personal pueda desarrollar las funciones asignadas, donde las necesidades de capacitación y formación sean cubiertas razonablemente.

2.4 Auditoría de Sistemas de Información

Existen diversos tipos de auditoría que pueden efectuarse tanto por personal interno de una organización, como personal externo. Entre los principales tipos se encuentran las auditorías de cumplimiento cuyo objetivo consiste en determinar si se cumple con el marco normativo organizacional o de la industria a la que pertenece; asimismo, las auditorías financieras tienen como propósito determinar la exactitud de los estados financieros. Por su parte, la auditoría operativa evalúa la estructura de control interno en un proceso o área específica de la organización.

Otro caso corresponde a la auditoría forense, cuya especialización consiste descubrir, revelar y hacer seguimiento a fraudes y crimines; De igual manera, cuando se habla de una auditoría integrada, se refiere a la combinación de pasos de auditoría operativa y financiera, con la finalidad de evaluar los objetivos generales del sujeto del estudio.

En lo que respecta a las auditorías de Sistemas de Información, tipo de auditoría que la Firma EEQA desea desarrollar como parte de su portafolio de servicios, se define como el proceso que *"recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y disponibilidad de los datos y del sistema, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan eficientemente los recursos y tienen en efecto controles internos que proveen una certeza razonable de que los objetivos del negocio, operacionales y de control serán alcanzados y que los eventos no deseados serán evitados o detectados y corregidos de forma oportuna."* (ISACA, 2015, pág. 45).

Dentro de la categorías de las auditorías de los Sistemas de Información, existen revisiones especializadas que examinan áreas específicas, tal es el caso de una auditoría destinada a evaluar la razonabilidad de un Sistema de Gestión de la Seguridad de la Información.

Por lo general, la ejecución de una Auditoría de Sistemas de Información con lleva la realización de las siguientes fases:

Cuadro No. 2: Fases de una Auditoría

Fase de la Auditoría	Descripción
Sujeto de la Auditoría	Identificar el área que será auditada.
Objetivo de la Auditoría	Identificar el propósito de la auditoría.
Alcance de la Auditoría	Identificar los sistemas, funciones o unidades específicos de la organización que serán incluidos en la revisión.
Planificación de Pre-Auditoría	-Identificar habilidades y recursos técnicos necesarios. -Identificar las fuentes de información para la prueba o examen (diagramas de flujo, políticas, normas, procedimientos y papeles de trabajo anteriores a la auditoria, entre otras) -Identificar las localidades o instalaciones que serán auditadas.
Procedimientos de Auditoría y pasos para la recolección de datos	-Identificar y seleccionar el enfoque de auditoría para verificar y comprobar los controles. -Identificar una lista de individuos que serán entrevistados. -Identificar y obtener las políticas, estándares y

Fase de la Auditoría	Descripción
	directrices departamentales para realizar la revisión. -Desarrollar herramientas y metodología de auditoría para probar y verificar el control.
Procedimientos para evaluar los resultados de la prueba o la revisión	Específico de la organización.
Procedimientos para la comunicación con la gerencia	Específico de la organización.
Preparación del reporte de auditoría	-Identificar los procedimientos de seguimiento de la revisión. -Identificar los procedimientos para evaluar/probar la eficiencia y efectividad operacional. -Identificar los procedimientos para probar los controles. -Revisar y evaluar la calidad de los documentos, políticas y procedimientos.

Fuente: (ISACA, 2015)

2.5 Otras definiciones en el ámbito de la Gestión de Proyectos

A continuación se incluye una serie de conceptos relevantes relacionados con la Dirección de Proyectos, los cuales son mencionados en el punto número 4 del presente documento:

Método PERT: Herramienta para la valuar la duración de las actividades de un proyecto, que utiliza tres estimaciones para definir un rango aproximado de duración de una actividad:

• **Más probable** (*tM*). Esta estimación se basa en la duración de la actividad, en función de los recursos que probablemente le sean asignados, de su productividad, de las expectativas realistas de disponibilidad para la actividad, de las dependencias de otros participantes y de las interrupciones.

• **Optimista** (*tO*). Estima la duración de la actividad sobre la base del análisis del mejor escenario posible para esa actividad.

• **Pesimista** (*tP*). Estima la duración de la actividad sobre la base del análisis del peor escenario posible para esa actividad. (PMI, 2013, pág. 176).

Ruta Crítica del Proyecto: Es un método analítico empleado como parte de la generación del cronograma para estimar la duración mínima del proyecto y determinar el nivel de flexibilidad en la programación de los caminos de red lógicos dentro del cronograma. Esta técnica de análisis de la red del cronograma calcula las fechas de inicio y finalización, tempranas y tardías, para todas las actividades, sin tener en cuenta las limitaciones de recursos, y realiza un análisis que recorre hacia adelante y hacia atrás toda la red del cronograma. (PMI, 2013, pág. 176).

3. MARCO METODOLOGICO

3.1 Fuentes de información

Las fuentes de información son todo aquello que suministre una noticia, una información o un dato, que pueda transmitir conocimiento. (López, 2017). Son de alta importancia para satisfacer una demanda de información o conocimiento, como lo sería el desarrollo del trabajo académico, profesional y científico.

Al considerar la enorme cantidad de datos existentes en la actualidad, es primordial efectuar una eficaz selección de las fuentes a partir de una concepción clara de los objetivos que se desean alcanzar, lo que permitirá mantener un equilibrio entre la calidad, cantidad y actualidad en las diferentes áreas de interés que forman parte del alcance de la investigación, además que se garantiza un adecuado balance temático.

Fueron diversas las fuentes de información consultadas para el desarrollo del presente trabajo, tanto en formato impreso como digital, principalmente relacionadas con marcos de referencia sobre las buenas prácticas para la gestión de las tecnologías de información, donde se brindó énfasis a la seguridad de la información.

3.1.1 Fuentes Primarias

Se determina que las fuentes primarias “proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes” (Hernández, 2014, pág.27). Para efectos de este trabajo, se establece como fuente primaria las entrevistas efectuadas al personal humano que conforma a la firma de consultoría EEQA.

3.1.2 Fuentes Secundarias

Las fuentes secundarias se refieren a “aquellos portadores originales de la información que no han retransmitido o grabado en cualquier medio o documento la información de interés” (Eyssautier, 2002).

Mediante el Cuadro No.3, se resumen las distintas fuentes de información que se utilizaron en este proyecto:

Cuadro No.3: Fuentes de Información Utilizadas

Objetivos	**Fuentes de información**	
	Primarias	**Secundarias**
Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional	-Reuniones individuales con algunos de los socios de la Firma EEQA, donde se analizaron los objetivos consignados en el Plan Estratégico para el periodo 2015-2020.	-Informe sobre la inversión extranjera directa en Costa Rica (2014), presentado por el Sr. José Rossi, presidente de la Junta Directiva de CINDE. -International Organization for Standardization. (2013). ISO/IEC 27001. Information technology - Security techniques - Information security management systems.
Elaborar un plan de gestión del cronograma	-Reunión con el Gerente de	Project Management Institute Inc (2011). Practice standard for

Objetivos	Fuentes de información	
	Primarias	**Secundarias**
para planificar, ejecutar y controlar las actividades del cronograma.	Auditoría de la Firma EEQA, donde se evaluó la razonabilidad de las actividades propuestas en el cronograma del proyecto, así como la disponibilidad de los recursos. -Documentos de proyectos anteriores, lecciones aprendidas.	scheduling second edition.
Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditor un sistema de gestión de seguridad de la información.	-Reunión con el Gerente General de la Firma EEQA, con la finalidad de revisar el presupuesto requerido para desarrollar el proyecto.	-Project Management Institute Inc. (2011). Practice standard for earned value management second edition. -Project Management Institute Inc. (2011). Practice standard for Project estimating.
Preparar un plan de gestión de la calidad	-Entrevista efectuada a	Lledó, Pablo. (2013). Director de proyectos: cómo aprobar el examen

Objetivos	Fuentes de información	
	Primarias	**Secundarias**
para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.	algunos miembros del equipo de auditores de la Firma EEQA, para identificar oportunidades de mejoras en relación con el desarrollo de los productos y servicios de auditoría. -Juicio experto.	PMP sin morir en el intento.
Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la Firma EEQA, que participará en el proyecto.	-Reunión con el encargado de recursos humanos de la Firma EEQA, con la finalidad de obtener información sobre las características del recurso humano de la firma.	Manual de Alumno del Curso ITIL Foundation versión 3.2.1, referente a la gestión de servicios de TI.
Generar un plan de gestión de	-Aplicación de encuesta para	Project Management Institute Inc. (2013). Guía de los fundamentos

Objetivos	Fuentes de información	
	Primarias	**Secundarias**
comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.	identificar oportunidades de mejora en relación con los canales de comunicación a lo interno de la firma. -Observación de herramientas de comunicación utilizadas por la firma.	para la dirección de proyectos (Guía PMBOK quinta edición).
Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.	-Revisión de la última valoración de riesgos efectuada por la firma. -Revisión de algunas matrices SEVRI, presentadas a la CGR.	-ISACA. (2016). Manual de Preparación para el examen CISM. -ISACA. (2016). Manual de Preparación para el examen CRISC -Acuerdo SUGEF 14-17. Reglamento General de Gestión de la Tecnología de Información (2017).
Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos	Revisión del inventario de herramientas y otros activos, el cual fue aportado	Contraloría General de la República. (2007). Normas técnicas para la gestión y el control de las Tecnologías de Información: Costa Rica.

Objetivos	Fuentes de información	
	Primarias	**Secundarias**
por el proyecto y los niveles de responsabilidad de las partes involucradas.	por la Firma EEQA.	
Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.	Análisis de la cartera de cliente de la Firma EEQA, con la finalidad de identificar beneficiados con el nuevo producto de auditoría.	ISACA. (2012). COBIT 5. Information Systems Audit and Control Association.

Fuente: (El Autor, 2018)

3.2 Métodos de Investigación

Los métodos de investigación son procedimientos ordenados que se siguen para establecer el significado de los hechos y fenómenos hacia los que se dirige el interés para encontrar, demostrar, refutar, descubrir y aportar al conocimiento. Existen muchas versiones de métodos, y en general implican procesos de análisis, síntesis, inducción y deducción. (Eyssautier, 2002).

3.2.1 Método Analítico-Sintético

“El estudio de los hechos, partiendo de la descomposición del objeto de estudio en cada una de sus partes para estudiarlas en forma individual (análisis), y luego se integran esas partes para estudiarlas de manera holística e integral (síntesis).” (Bernal, 2010)

3.2.2 Método Inductivo-Deductivo

“La inferencia se basa en la lógica y estudia hechos particulares, aunque es deductivo en un sentido (parte de lo general a lo particular) e inductivo en sentido contrario (va de lo particular a lo general).” (Bernal, 2010)

En el cuadro No. 4, se puede apreciar los métodos de investigación que se van a emplear para el desarrollo de los objetivos definidos para este proyecto.

Cuadro No.4: Métodos de Investigación Utilizadas

Objetivos	**Métodos de investigación**	
	Método Analítico-Sintético	**Método Inductivo-Deductivo**
Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto	El plan de gestión del alcance se subdivide en distintas secciones, con la finalidad de identificar los requerimientos del proyecto y formular los paquetes de trabajo y la EDT.	Identificar las actividades necesarias que corresponden a cada etapa del proyecto.

Objetivos	Métodos de investigación	
	Método Analítico-Sintético	**Método Inductivo-Deductivo**
en el ámbito nacional como internacional.		
Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.	Determinar las actividades que deben conformar al cronograma del proyecto y la secuencia correspondiente.	Identificar los mecanismos de control para el seguimiento del cumplimiento del cronograma.
Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditor un sistema de gestión de seguridad de la información.	Analizar los insumos requeridos para completar cada uno de los entregables del proyecto.	Estimar los costos requeridos para la implementación del proyecto.
Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.	Determinar los requerimientos y métricas de calidad para cada uno de los entregables.	Establecer los controles idóneos para monitorear la calidad del proyecto.
Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la	Identificar y documentar formalmente, los roles y las responsabilidades de los involucrados en el proyecto.	Seguimiento al desempeño del recurso humano del proyecto.

Objetivos	Métodos de investigación	
	Método Analítico-Sintético	**Método Inductivo-Deductivo**
Firma EEQA, que participará en el proyecto.		
Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.	Identificar las partes interesadas del proyecto y determinar los requerimientos de comunicación.	Se establecen los medios para la trasmisión oportuna de la información del proyecto.
Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.	Identificar, evaluar y documentar los riesgos inherentes al proyecto.	Establecer las medidas para gestionar los riesgos identificados del proyecto.
Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas.	Evaluar los requerimientos de los proveedores del proyecto, de conformidad al marco normativo establecido y al cronograma de actividades.	Definir herramientas para controlar las adquisiciones.
Elaborar un plan de gestión de los interesados para determinar las	Desarrollar la identificación de los interesados en la implementación del	Determinar los intereses y expectativas de las partes interesadas del proyecto.

Objetivos	Métodos de investigación	
	Método Analítico-Sintético	Método Inductivo-Deductivo
necesidades acorde con los roles establecidos.	proyecto.	

Fuente: (El Autor, 2018)

3.3 Herramientas

Para el desarrollo del presente proyecto se aplicarán una serie de técnicas y herramientas descritas en la quinta edición de la guía PMBOK formulada por el PMI (2013), con la finalidad de alinear la ejecución de cada una de las actividades establecidas en el plan de implementación con las buenas prácticas para la gestión de proyectos, las cuales se caracterizan por la amplia aceptación que ostentan a nivel mundial.

De esa forma, existirán mayores posibilidades de completar el proyecto de conformidad con todas las restricciones contrapuestas que se han definido.

En el cuadro N° 5 se definen las herramientas a utilizar para cada objetivo propuesto.

Cuadro No.5: Herramientas Utilizadas

Objetivos	Herramientas
Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los	-Análisis de Documentos -Análisis de Producto -Análisis de Variaciones -Cuestionarios y Encuestas

Objetivos	Herramientas
requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional.	-Descomposición -Entrevistas -Juicio Experto -Observaciones -Reuniones -Técnicas Grupales de Toma de Decisiones
Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.	-Análisis de Alternativas -Análisis de la Red del Cronograma -Descomposición -Juicio de Expertos -Método de la Ruta Crítica -PERT -Reuniones -Revisiones de Desempeño -Software de Gestión de Proyectos -Técnicas de Optimización de Recursos -Toma de Decisiones Grupales
Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información.	-Análisis de Oferta de Proveedores -Análisis de Reservas -Costos de Calidad -Gestión del Valor Ganado -Juicio Experto -Revisiones de Desempeño -Software de Gestión de Proyectos -Reuniones -Técnicas Analíticas -Toma de Decisiones Grupales
Preparar un plan de gestión de la	-Análisis de Costo-Beneficio

Objetivos	Herramientas
calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.	-Análisis de Procesos -Herramientas de Gestión de Calidad -Herramientas de Control de Calidad -Reuniones
Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la firma EEQA, que participará en el proyecto.	-Actividades de Equipo -Adquisiciones -Análisis de Decisiones Multicriterio -Evaluaciones de Desempeño del Proyecto -Habilidades Interpersonales -Herramientas de Evaluación Personal -Juicio Experto -Observación y Conversación -Organigramas y Descripciones de Cargos -Reuniones
Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.	-Análisis de Requisitos de Comunicación -Juicio Experto -Métodos de Comunicación -Modelos de Comunicación -Reuniones -Sistemas de Gestión de la Información -Tecnología para la Comunicación
Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente	-Análisis Listas de Verificación -Análisis Cuantitativos de Riesgo -Análisis de Supuestos -Análisis de Reservas

Objetivos	Herramientas
los riesgos vinculados con la función de TI.	-Categorización de los Riesgos -Estrategias de Respuestas de Contingencias -Estrategias para Riesgos Negativos o Amenazas -Evaluación de Urgencia del Riesgo -Evaluación de Probabilidad e Impacto de los Riesgos -Evaluaciones al Riesgo -Juicio Experto -Matriz de Probabilidad e Impacto -Reuniones -Revisiones a la Documentación
Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas.	-Análisis de Hacer o Comprar -Juicio Experto -Negociaciones de Adquisiciones -Reuniones -Revisiones al Desempeño de las Adquisiciones -Sistemas de Control de Cambios a Contratos -Sistema de Gestión de Registro -Sistemas de Pago -Técnicas de Evaluación de Propuestas
Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.	-Análisis de Interesados -Habilidades de Gestión -Habilidades Interpersonales -Juicio Experto -Métodos de Comunicación

Objetivos	Herramientas
	-Reuniones -Sistemas de Gestión de la Información

Fuente: (El Autor, 2018)

3.4 Supuestos y Restricciones

La quinta edición de la Guía PMBOK (PMI, 2013) define a los Supuestos como "factores del proceso de planificación que se consideran verdaderos, reales o seguros sin pruebas ni demostraciones".

Por su parte las Restricciones corresponden según PMBOK (PMI, 2013) a "factores limitantes que afectan la ejecución de un proyecto o proceso". Los Supuestos y Restricciones y su relación con los objetivos del proyecto final de graduación se ilustran a continuación en el cuadro No.6:

Cuadro No.6: Supuestos y Restricciones

Objetivos	Supuestos	Restricciones
Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas	- Se cuenta con el apoyo de los socios de la firma de consultoría, quienes conforman el órgano director. - Durante el 2017 se recibió 4 invitaciones para participar	Por limitación del presupuesto y del plan estratégico de la Firma EEQA, este proyecto toma en cuenta únicamente la etapa de formulación de la propuesta, por lo que la implementación final se

Objetivos	Supuestos	Restricciones
practicas, tanto en el ámbito nacional como internacional.	en procesos concursales, donde se determinaban las especificaciones técnicas y condiciones generales del servicio de auditoría requerido por el cliente, lo cual se convierte en un valioso activo para formular el plan del alcance del proyecto.	desarrollará en otro momento, previo acuerdo de los Socios de la Firma.
Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.	El “Juicio Experto” que ostentan los involucrados en el proyecto, hace prever que la estimación de la duración de las actividades del cronograma, será razonable.	Únicamente se cuenta con tres meses para la formulación y entrega de la propuesta del plan para auditar un Sistema de Gestión de Seguridad de la Información (SGSI).
Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información.	Los socios de la de la Firma EEQA, han manifestado reiteradamente el soporte económico para la realización del proyecto; asimismo, se cuenta con la experiencia suficiente en el equipo de proyecto para estimar correctamente el costo de las actividades.	La compra de las licencias para el uso de las herramientas tecnológicas que se implementarán como parte del plan para auditar un SGSI, no puede sobrepasar los $ 5.000 anuales. Se descarta la posibilidad de efectuar modificaciones presupuestarias para realizar compras superiores al monto indicado.

Objetivos	Supuestos	Restricciones
Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.	Las buenas prácticas referente a la calidad en la ejecución de las auditorías son aplicables a todas las evaluaciones independientemente de su naturaleza, sean estas financieras, operativas o de tecnologías de información.	Los estándares de calidad de la auditoría a implementar, obligatoriamente deben alinearse con las buenas prácticas consignadas en el marco de referencia COBIT 5, el estándar de seguridad ISO-27001 y con la metodología ITIL v3.
Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la Firma EEQA, que participará en el proyecto.	- Los objetivos del proyecto han generado mucho interés de parte del equipo de auditores de la firma y existen altas expectativas, por lo que se proyecta una activa participación de parte del recurso humano de la firma. - El recurso humano cuenta con un robusto conocimiento en el campo de la auditoria, lo que beneficiará el desarrollo del proyecto.	Las directrices emitidas por el Director del Proyecto para dirigir los esfuerzos del personal que participa del proyecto, no pueden entrar en conflicto con el Marco Normativo que ha establecido la Firma EEQA.
Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del	Se considera que el flujo de la información entre el personal de la firma involucrado en el proyecto es eficaz, donde además	- La metodología para el manejo de la información y de la documentación de la misma, no se encuentra del todo orientada a la gestión

Objetivos	Supuestos	Restricciones
proyecto.	prevalecen criterios de confidencialidad y objetividad en relación con la manipulación de la información.	de proyectos, por lo que será necesario adoptar buenas prácticas del PMI. - Existen canales autorizados específicamente por la Firma EEQA, que tienen la potestad de hacer pública la información de la firma, por lo que será necesario contactar inicialmente a estas fuentes para la solicitud de información.
Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.	- La identificación y valoración de riesgos es una de las principales fortalezas de las firmas de auditoría, por lo que se pronostica una activa participación en este entregable por parte de la consultora EEQA. -Se establece una reserva de contingencia necesaria para atender los riesgos del proyecto.	Debido a la limitación del presupuesto del proyecto, no existe la posibilidad de transferir el riesgo a terceros mediante el pago de un seguro.
Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por	-Los productos o servicios requeridos por el proyecto, se entregarán de conformidad con las	Dependiendo del monto de las adquisiciones necesarias para el desarrollo del proyecto, estas pueden ser

Objetivos	Supuestos	Restricciones
el proyecto y los niveles de responsabilidad de las partes involucradas.	condiciones pactadas con los proveedores.	aprobadas por la Gerencia de Auditoría, la Gerencia General o los Socios de la firma, según corresponda.
Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.	Existe compromiso de parte de los interesados del proyecto, de participar activamente en el desarrollo del mismo; de igual forma, el conocimiento que ostenta los recursos involucrados, impactará positivamente al proyecto.	La estructura organizacional de la Firma EEQA, no posibilita que sus funcionarios tengan una dedicación del %100 al proyecto, ya que la atención de los clientes es prioritaria.

Fuente: (El Autor, 2018)

3.5 Entregables

Los entregables corresponden a “cualquier producto medible o verificable que se elabora para completar un proyecto o fase de él” (Esterkin, 2010). Por consiguiente, un entregable puede ser un objeto tangible o no que es suministrado a una parte interna o externa del proyecto. En el cuadro No.7 se definen los entregables para cada objetivo propuesto.

Cuadro No. 7: Entregables

Objetivos	Entregables
Desarrollar un plan de gestión del alcance para identificar las actividades	**Plan de Gestión del Alcance:** Detalla cómo se va a definir, validar y controlar

Objetivos	Entregables
necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional.	el alcance del proyecto. Contiene los procedimientos necesarios para gestionar los cambios en el alcance. **Plan de Gestión de los Requisitos:** Describe cómo se analizarán, documentarán y gestionarán los requisitos del proyecto. **Estructura de Desglose de Trabajo:** Corresponde al proceso de subdividir los entregables y el trabajo del proyecto en componentes más pequeños y más sencillos de manejar.
Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.	**Plan de Gestión del Cronograma:** Define la forma en que se informará sobre las contingencias relativas al cronograma y la forma en que se evaluarán las mismas. **Lista de Actividades:** Incluye todas las actividades del cronograma necesarias para el proyecto; asimismo, considera para cada actividad su identificador de la misma y una descripción del alcance del trabajo. **Atributos de las Actividades:** Amplían la descripción de la actividad, al identificar los múltiples componentes relacionados con cada una de ellas. Los componentes de cada actividad evolucionan a lo largo del tiempo.

Objetivos	Entregables
	Lista de Hitos: Se identifican todos los hitos del proyecto y se indica si éstos son obligatorios, como los exigidos por contrato, u opcionales, como los basados en información histórica. Los hitos son similares a las actividades normales del cronograma, presentan idéntica estructura e idénticos atributos, pero tienen una duración nula, ya que representan un momento en el tiempo. **Diagramas de Red del Cronograma del Proyecto:** Representación gráfica de las relaciones lógicas, también denominadas dependencias, entre las actividades del cronograma del proyecto. **Recursos Requeridos para las Actividades:** Consiste en los tipos y las cantidades de recursos identificados que necesita cada actividad de un paquete de trabajo. **Estructura de Desglose de Recursos:** Es una representación jerárquica de los recursos por categoría y tipo, siendo de utilidad para organizar y comunicar los datos del cronograma del proyecto, junto con información sobre la utilización de recursos. **Cronograma del Proyecto:** Presenta

Objetivos	Entregables
	actividades relacionadas con fechas planificadas, duraciones, hitos y recursos. Debe contener, como mínimo, una fecha de inicio y una fecha de finalización planificadas para cada actividad.
Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información.	**Plan de Gestión de los Costos:** Describe la forma en que se planificarán, estructurarán y controlarán los costos del proyecto. **Estimación del Costo de las Actividades:** Se utilizan para evaluar cuán razonables son las ofertas y propuestas recibidas de los vendedores potenciales **Líneas Base de Costos:** Es la versión aprobada del presupuesto por fases del proyecto y se utiliza como base de comparación con los resultados reales.
Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.	**Plan de Gestión de la Calidad:** Describe los enfoques del aseguramiento de la calidad y de la mejora continua de procesos para el proyecto. **Métricas de Calidad:** Describe de manera específica un atributo del producto o del proyecto, y la manera en que lo medirá el proceso de control de calidad.

Objetivos	Entregables
Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la firma EEQA, que participará en el proyecto.	**Plan de Gestión del Recurso Humano:** Consigna las responsabilidades, las habilidades requeridas y las relaciones de comunicación, así como de crear un plan para la gestión de personal. **Evaluaciones de Desempeño:** Posibilitan el establecer acciones para resolver los incidentes o asuntos, hacer ajustes en la comunicación, abordar los conflictos y mejorar la interacción del equipo del proyecto.
Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.	**Plan de Gestión de las Comunicaciones:** Permite el administrar las necesidades y los requisitos de información de los interesados y de los activos de la organización disponibles.
Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.	**Plan de Gestión del Riesgo:** Describe el modo en que se estructurarán y se llevarán a cabo las actividades de gestión de riesgos. **Registro de Riesgos:** Es un documento en el cual se registran los resultados del análisis de riesgos y de la planificación de la respuesta a los riesgos.
Desarrollar un plan de gestión de adquisiciones para identificar los flujos	**Plan de Gestión de las Adquisiciones:** Describe cómo un

Objetivos	Entregables
de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas.	equipo de proyecto adquirirá bienes y servicios desde fuera de la organización ejecutora. **Criterios de Selección de Recursos:** Conjunto de atributos requeridos por el comprador, los cuales debe satisfacer o superar a fin de ser seleccionado para un contrato. **Acuerdos:** Definen las intenciones iniciales de un proyecto. Algunos ejemplos son los contratos, memorandos de entendimiento (MOUs), acuerdos de nivel de servicio (SLA), cartas de acuerdo, declaraciones de intenciones, acuerdos verbales, correos electrónicos u otros acuerdos escritos.
Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.	**Plan de Gestión de los Interesados:** Proceso de desarrollar estrategias de gestión adecuadas para lograr la participación eficaz de los interesados a lo largo del ciclo de vida del proyecto, con base en el análisis de sus necesidades, intereses y el posible impacto en el éxito del proyecto. **Registro de los Interesados:** Proporciona detalles sobre los participantes en el proyecto y sus intereses en el mismo.

Objetivos	Entregables
	Registro de Incidentes: Este registro se actualiza a medida que se identifican nuevos incidentes y se resuelven los incidentes actuales que puedan presentarse entre los interesados del proyecto.

Fuente: (El Autor, 2018)

4. DESARROLLO

4.1 Gestión de la Integración del Proyecto

La Gestión de la Integración del Proyecto *"incluye los procesos y actividades necesarias para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de dirección del proyecto dentro de los Grupos de Procesos de la Dirección de Proyectos"* (PMI, 2013, pág. 63), incrementando con ello el control sobre el proyecto, lo que implica la toma de decisiones de modo que el proyecto se complete según lo planificado. Cabe destacar la relevancia del Acta de Constitución del Proyecto, documento que autoriza formalmente su existencia y que concede a su director la autoridad para asignar los recursos de la organización a las actividades del proyecto; no obstante, dicho documento debe formularse previo al inicio de la planificación del proyecto, por lo que no puede considerarse como parte del desarrollo del "Plan de Dirección del Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Firma de Consultoría EEQA"

Asimismo, en lo que respecta al presente proyecto, dicho documento se elaboró a partir de la información obtenida de las sesiones de trabajo efectuadas con los

Socios de la firma EEQA, con el Gerente de Auditoría y con algunos otros miembros de su personal, lo que permitió identificar los objetivos, los requisitos, los supuestos y las restricciones, entre otros aspectos claves del proyecto a desarrollar.

Cuadro No. 8: Acta del Proyecto

ACTA DEL PROYECTO	
Fecha	**Nombre de Proyecto**
06/11/2017	Plan de Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para la Firma de Consultoría EEQA.
Areas de conocimiento / procesos:	**Area de aplicación (Sector / Actividad):**
Grupos de Procesos: Iniciación, planificación. **Áreas de Conocimiento:** Integración, alcance, plazo, costo, calidad, riesgos, comunicaciones, recursos humanos, adquisiciones e interesados.	Consultoría. Auditoría. Tecnologías de Información.
Fecha de inicio del proyecto	**Fecha tentativa de finalización del proyecto**
19/02/2018	15/06/2018
Objetivos del proyecto (general y específicos)	
Objetivo general Crear una propuesta de un plan de dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para que la Firma Consultora EEQA pueda implementarlo como parte de su cartera de servicios profesionales. **Objetivos específicos** 1. Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas practicas, tanto en el ámbito nacional como internacional. 2. Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del proyecto. 3. Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un sistema de gestión de seguridad de la información. 4. Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio. 5. Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la Firma EEQA, que participará en el proyecto. 6. Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto. 7. Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI. 8. Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas. 9. Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos. 10. Desarrollar un formulario que contenga una lista de actividades que deben formar parte del plan para evaluar la	

razonabilidad del Sistema de Gestión de Seguridad de la Información implementado por los clientes de la Firma EEQA, considerando para ello los criterios de integridad, confidencialidad y disponibilidad de la información.

Justificación o propósito del proyecto (Aporte y resultados esperados)

La información es un recurso invaluable para que las organizaciones puedan tomar decisiones, continuar operando y alcanzar sus objetivos estratégicos; asimismo, otro aspecto destacable es el auge de la tecnología como medio para su administración.

Al respecto, es lógico determinar el incremento de los riesgos y amenazas contra la integridad, disponibilidad y confidencialidad de la información, por lo que la implementación de un Sistema de Gestión de Seguridad de la Informacion, es una buena práctica para adoptar controles de orden preventivo y correctivo que permitan dar respuesta al robo de datos, brechas de seguridad y ataques cibernéticos, entre otros eventos.

La consultora EEQA es una firma radicada en Costa Rica, que actualmente se especializa en la prestación de servicios contables, lo cual incluye auditorías para determinar la razonabilidad de los estados financieros. EEQA es considerada una firma menor, cabe indicar que en Costa Rica tienen presencia las 4 consultoras más grandes del mundo: PWC, Ernst & Young, KPMG y Deloitte. A pesar de ello, la firma ha logrado consolidar una importante cartera de clientes; sin embargo, algunas oportunidades de negocios han sido desaprovechadas debido a que EEQA no ostenta como parte de su catálogo de servicios, asesorías sobre la gestión de las tecnologías de información, en su nómina tampoco figura algún profesional experto en dicha temática.

Por consiguiente, la firma desea desarrollar su propio plan de auditoría que le permita asesorar a sus clientes en relación con el estado actual del "Sistema de Gestión de Seguridad de la Información", de igual forma, generar nuevas oportunidades de negocio e incrementar los niveles de ingreso y rentabilidad. Es relevante indicar que existen diferentes marcos metodológicos y buenas prácticas que servirán de insumo al proyecto para formular una propuesta de auditoría cuya implementación sea viable comercializar.

Descripción del producto o servicio que generará el proyecto – Entregables finales del proyecto

El producto final del proyecto es un documento con una propuesta de un plan de dirección de un proyecto para auditar un "Sistema de Gestión de Seguridad de la Información", que considere el gobierno de seguridad de la información, la gestión de riesgos de la información y su cumplimiento, el desarrollo y la gestión del programa de seguridad de la información y la gestión de incidentes.

Los entregables que lo conforman son los planes de gestión de las 10 áreas de conocimiento consignadas en la quinta edición de la Guía de Fundamentos PMBOK, para lo cual se formularan las plantillas respectivas.

Finalmente, se creará un formulario que contenga la lista de actividades que deben formar parte del plan para auditar un Sistema de Gestión de Seguridad de la Información.

Supuestos

El personal de la firma consultora suministrará información veraz en relación con las necesidades identificadas; asimismo, no existe resistencia en lo concerniente a incursionar en el asesoramiento de tecnologías de información.
El plazo establecido para efectuar el plan de proyecto es razonable y permitirá alcanzar los resultados planificados.
La calidad de la información existente es adecuada y pertinente para poder realizar los planes gestión del proyecto e identificar oportunidades de mejora.
No habrá ningún tipo de inconveniente durante el proceso de inscripción de la Firma EEQA, en el registro de oferentes de la SUGEF.

Restricciones

El plazo para finalizar el proyecto termina el 15 de junio de 2018.
La firma consultora EEQA carece de experiencia en relación con la ejecución de auditorías en el ámbito de las tecnologías de información.

Existe en Costa Rica un Marco Normativo de acatamiento obligatorio, que incluye las normas técnicas para la gestión y el control de las tecnologías de información y el acuerdo de la SUGEF 14-17 correspondiente al reglamento de gestión de las

tecnologías de información, entre otros, los cuales son documentos que deben ser considerados al formular un plan de auditoría aplicable en Costa Rica.

Identificación riesgos

1. Si la Firma Consultora EEQA no proporciona la información necesaria para el proyecto, podría afectar su alcance, el presupuesto y la calidad final del documento.
2. Las tecnologías de información se caracterizan por su dinamismo, por lo que nuevos requerimientos principalmente desde la perspectiva de seguridad, pueden originar modificaciones a la propuesta de auditoría.
3. El desconocimiento e inexperiencia en el tema tecnológico por parte de algunos miembros de la Firma EEQA, principalmente de quienes toman decisiones, podría generar desinterés en la implementación del proyecto, máxime si el mismo adquiere mayor complejidad conforme su desarrollo avanza.
4. De incrementarse el costo de la implementación de la propuesta, podría afectarse su implementación como parte de la cartera de servicios de la Firma Consultora EEQA.

Presupuesto

Descripción	Monto
Contratación de Asesor Experto en Seguridad Informática.	$ 2.000
Contratación del Director del Proyecto.	$ 2.300
Horas de Trabajo del equipo de Auditores	$ 12.400
Horas de Trabajo del equipo Administrativo	$ 6.300
Curso de Fundamentos ITIL para la gestión de servicios de TI	$ 750
Libro Manual de Revisión CISM, formulado por ISACA	$ 140
Servicios de Telecomunicaciones (Internet)	$ 100
Telefonía Celular	$ 100
Kilometraje	$ 200
Reservas	$ 2.183
Actividades para la prevención y corrección de desviaciones del Plan del Proyecto	$ 2.488
Total	**US$ 28.961**

Principales hitos y fechas

Nombre hito	Fecha inicio	Fecha final
Identificación de Requisitos del Proyecto	19 de febrero de 2018	21 de febrero de 2018
Especificación del Marco Normativo	22 de febrero de 2018	26 de febrero de 2018
Implementación de Herramientas Tecnológicas	27 de febrero de 2018	16 de marzo de 2018
Elaboración y Formalización de Procedimientos de Auditoría	19 de marzo de 2018	13 de abril de 2018
Definición de Herramienta para la Valoración de Riesgos de TI	16 de abril de 2018	20 de abril de 2018
Gestión del Recurso Humano	23 de abril de 2018	24 de abril de 2018
Creación del Plan de Revisión de los recursos de TI, desde la perspectiva de seguridad	25 de abril de 2018	31 de mayo de 2018

Entrega del Proyecto	04 de junio de 2018	06 de junio de 2018

Información histórica relevante

La Firma de Consultoría EEQA nace como parte de la iniciativa de un grupo de profesionales en contaduría pública y auditoría, con amplia experiencia en Costa Rica. Entre sus servicios profesionales se encuentran las auditorías financieras, servicios contables, certificaciones de ingreso, elaboración de planillas y control interno.

Sus oficinas centrales se localizan en la provincia de San José y figuran como sus principales clientes empresas del sector automovilístico y de logística de servicios de transporte. Recientemente, EEQA implementó los servicios de asesoría legal y su siguiente paso como parte de su estrategia de crecimiento, consiste en la incursión en el campo de las Tecnologías de Información.

El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), mediante artículo 6, del acta de la sesión 773-2009 del 20 de febrero del 2009 aprobó el Acuerdo SUGEF 14-09 "Reglamento sobre la gestión de la tecnología de información", que define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras (SUGEF). Asesorar a entidades financieras que deben cumplir con la norma supra citada, motivó a la Firma EEQA a desarrollar su propia propuesta de auditoría para aplicarla comercialmente.

Identificación de grupos de interés (involucrados)

Involucrados directo(s):
Socios de la Firma EEQA.
Auditores Senior de la Firma EEQA.
Auditores Junior de la Firma EEQA.
Clientes de la Firma EEQA.
Director del Proyecto.
Asesor experto en Seguridad Informática.

Involucrados indirecto(s):
Superintendencia General de Entidades Financieras (SUGEF).
Contraloría General de la República (CGR).
Clientes de la Firma EEQA.

Director de proyecto: **Maikol Fernando Hernández Segura**	**Firma:**
Autorización de:	**Firma:**

Fuente: (El Autor, 2018)

Al indicar que el proyecto busca desarrollar una propuesta de auditoría, lo que se pretende es que la Firma EEQA, identifique, evalúe y seleccione aquellos estándares, buenas prácticas y herramientas tecnológicas existentes en el mercado, que le permitan estructurar un plan para auditar un Sistema de Gestión de la Seguridad de la Información, que tenga potencial para ser comercializado entre sus clientes.

Lo anterior implica diseñar papales de trabajo cuyo grado de especificación le permita a la Firma EEQA el evaluar la razonabilidad de la gestión de la infraestructura de tecnologías de información; ejemplo de ello son los cuestionarios, guías para entrevistas y listas de chequeo, entre otros instrumentos, que servirán para ejecutar pruebas de cumplimiento y pruebas sustantivas mediante las cuales se recabará evidencia competente y suficiente para generar oportunamente, hallazgos y recomendaciones objetivas.

Entre los documentos que se constituirán como activos para la Firma EEQA específicamente en lo concerniente a la gestión de proyectos, se encuentran los formularios para la Solicitud de Cambios, cuya finalidad es documentar la trazabilidad que ostenta un cambio desde su origen hasta su conclusión; asimismo, se propone un documento complementario tipo bitácora que registra un histórico de todos los cambios implementados en el proyecto, lo que sin duda aporta información relevante a las distintas partes interesadas. Los cambios propuestos serán evaluados y autorizados por el Consejo Asesor de Cambios (CAB), integrado por los Socios de la Firma EEQA, el Gerente de Auditoría y por el Director del Proyecto. A continuación, se adjuntan los formularios a utilizar en el proyecto “Plan de Dirección de un Proyecto para auditar un Sistema de Gestión de Seguridad de la Información (SGSI):

Cuadro No. 9: Formulario Solicitud de Cambio

Solicitud de Cambio		
Firma Consultora EEQA		
Información del Proyecto		
Fecha:	**Nombre del Proyecto:**	**Identificación del Proyecto:**
	Plan de Dirección para auditar un Sistema de Gestión de Seguridad de la Información	
Cambio Solicitado		
Área o Departamento que solicita el cambio:	**Persona que solicita el cambio:**	
Descripción del Cambio:		

Causa del Cambio:
Requerimiento Legal o regulatorio:
Nueva Necesidad:
Omisión de Requerimiento:
Atrasos de acuerdo a lo planificado:
Ajustes para mejora, definido durante la ejecución del proyecto:
Otro:
Descripción del Cambio:

Firmas de control		
Persona que solicita el cambio:		
Nombre	**Cargo**	**Firma**
Aprobación del Encargado o Jefatura del Área Funcional:		
Nombre	**Cargo**	**Firma**

<u>Análisis del Impacto del Cambio Solicitado</u>		
Descripción del Impacto:		
Afectación		
Tiempo:		
Recursos:		
Presupuesto y costos estimados:		
Impacto Técnico:		
Impacto en otros Proyectos:		
Fecha estimada para la implementación del cambio:		
Análisis efectuado por el Comité de Control de Cambios:		
Aprobado ( ) Rechazado ( ) Denegado ( ) Requiere aprobación del Patrocinador ( )		
Nombre	**Cargo**	**Firma**

<u>Autorización Final por parte del Patrocinador</u>

Aprobado ( )	Rechazado ( )	Denegado ( )
Nombre	**Cargo**	**Firma**

Fuente: (El Autor, 2018)

Cuadro No. 10: Formulario Bitácora de Cambios

Bitácora de Cambios del Proyecto								
Firma Consultora EEQA								
Información del Proyecto								
Fecha:	**Nombre del Proyecto:**			**Identificación del Proyecto:**				
	Plan de Dirección para auditar un Sistema de Gestión de Seguridad de la Información							
Bitácora								
Número	**Descripción del Cambio**	**Fecha de Solicitud**	**Solicitado por**	**Fecha de Atención**	**Resolución**	**Impacto**	**Autoriza**	**Estado**
Elaborado por: **Fecha :**								

Fuente: (El Autor, 2018)

4.2 Plan de Gestión del Alcance

La declaración del alcance describe detalladamente los entregables y todo el trabajo necesario para llevarlos a cabo; partiendo de ello, se procede a desarrollar la matriz de trazabilidad de los requisitos. Esta matriz se representa en un cuadro

y ayuda a vincular los requisitos del producto desde que se originan hasta los entregables que los satisfacen (PMI, 2013).

Cuadro No. 11: Requisitos Identificados por el Personal de la Firma EEQA

ID	Requisito	Descripción	Prioridad	Criterio de Aceptación
001	Alineación con las buenas prácticas y marcos de referencia de TI	La propuesta de auditoría a desarrollar debe permitir evaluar el grado de madurez en la aplicación de buenas prácticas por medio del marco de referencia de los Objetivos de Control de COBIT y la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL).	Alta	Implementación de instrumentos tales como cuestionarios y listas de chequeo, para la valoración de los marcos de referencia de TI.
002	Flexibilidad de aplicación independietemente del segmento de negocios al que pertenece el cliente	No debe exitir limitaciones en la aplicación del plan de auditoría a desarrollar. El mismo podrá ser aplicada en organizaciones sin importantar su dimensión o su giro	Alta	Procedimientos de auditoría que formalicen los lineamientos para el desarrollo de los estudios de auditoría y para la definición de los recursos requeridos para su

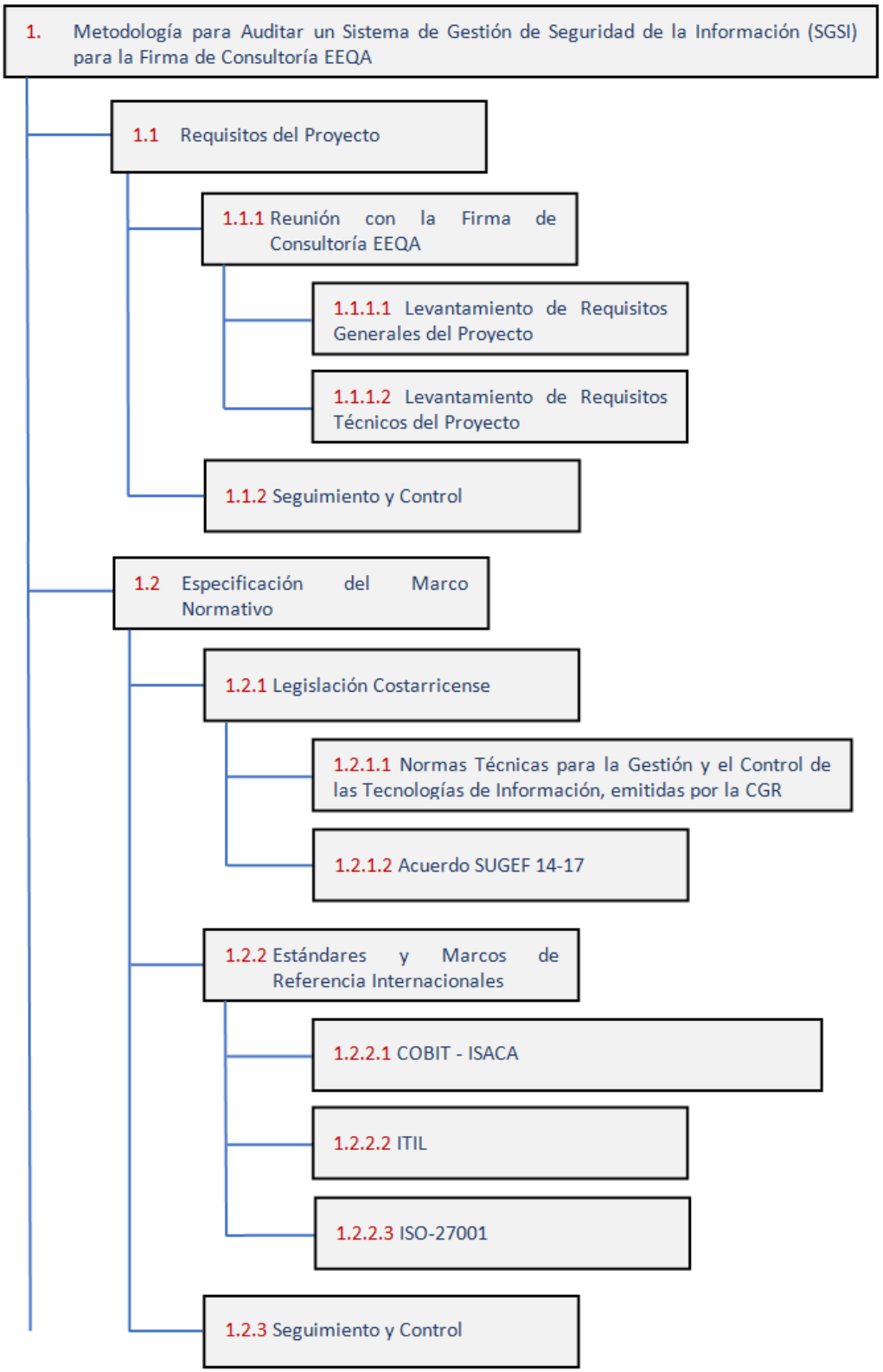
ID	Requisito	Descripción	Prioridad	Criterio de Aceptación
		de negocios.		ejecución.
003	Incorporación de herramientas tecnológicas	El plan de auditoría a implementar debe permitir la incorporación de herramientas tecnológicas que suministren mayor profundidad a la auditoría, así como la automatización de tareas.	Alta	Adquisición e implementación de al menos una herramienta para el análisis de datos; asimismo, se deben incorporar herramientas para identificar vulnerabilidades de servidores, bases de datos y en la infraestructura de telecomunicaciones.
004	Instrumento para la valoración de riesgos	Se debe incorporar como parte del plan de auditoría, un instrumento para la evaluación cualitativa y cuantitativa del riesgo vinculado con la gestión de las tecnologías de información.	Alta	Los instrumentos para la valoración de riesgos se deben basar en un razonamiento sólido, auditable y de conformidad con el marco regulatorio nacional.
005	Capacitar al personal de auditoría en temas relacionados con las tecnologías de	Entre las capacitaciones propuestas, se encuentran COBIT 5,	Alta	Creación de un plan integral de capacitación de personal, acorde con

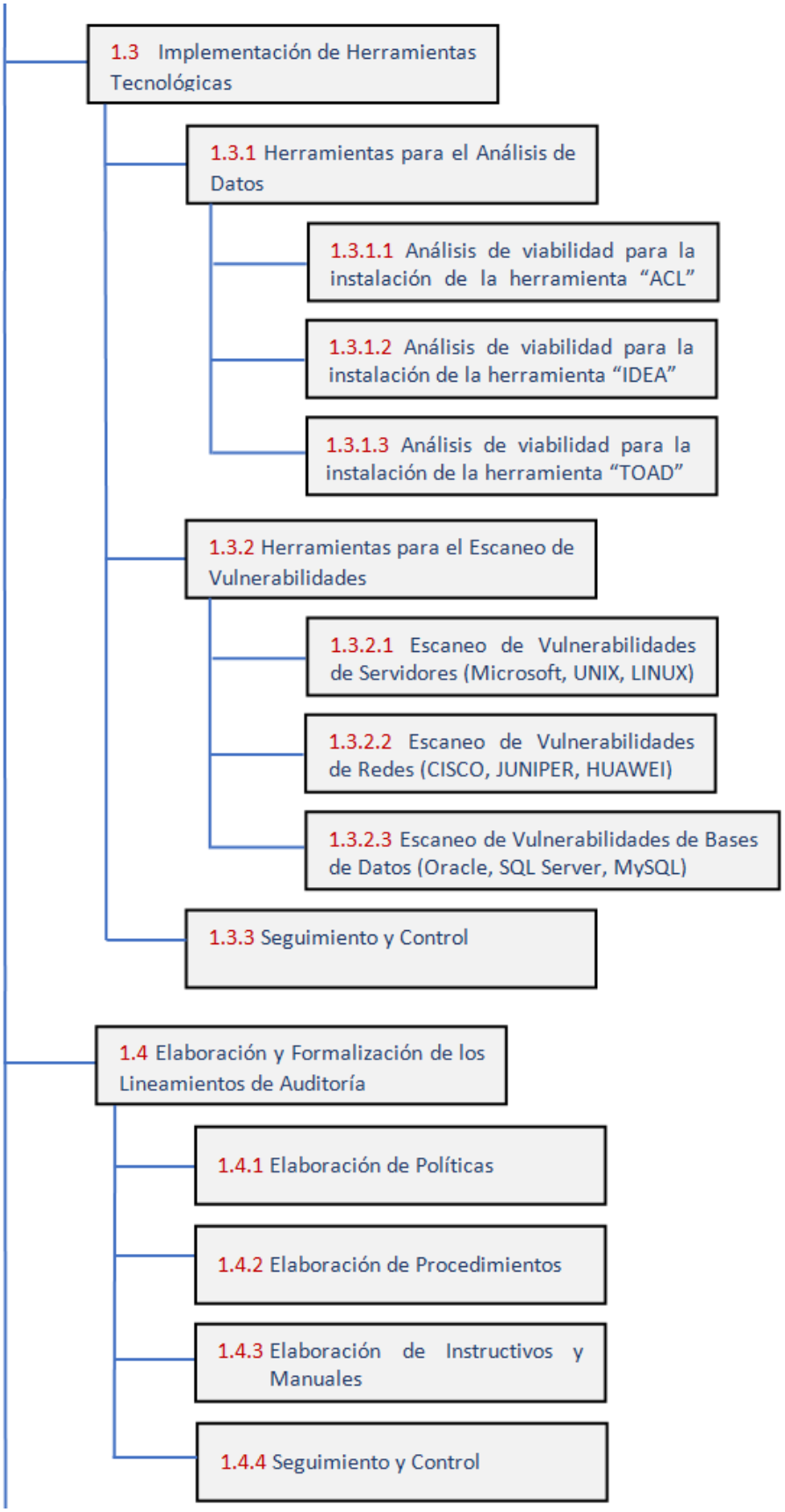
ID	Requisito	Descripción	Prioridad	Criterio de Aceptación
	información	ISO 27001 e ITIL v3. Estos marcos permiten el desarrollo del enfoque de supervisión basado en riesgos.		las necesidades en materia de tecnologías de información que han externado los clientes de la firma EEQA.
006	Obtención de certificaciones de seguridad informática y de gestión de TI	La industria y los profesionales en TI, han desarrollado estándares y marcos que permiten gestionar y controlar las tecnologías. La obtención de certificaciones internacionales tiene repercusión en la reputación de la firma.	Media	Obtención de certificaciones tales como ITIL, CISA, CISM y CRISC, entre otras.
007	Evaluación de la Norma 14-17 SUGEF	Se debe proporcionar la capacitación necesaria al personal de la firma, para la evaluación de la Norma 14-17 emitida por la SUGEF, por cuanto las entidades	Alta	Formar parte del Registro de Auditores elegibles de la SUGEF. De esta forma, la firma EEQA se encontrará habilitada para participar como

ID	Requisito	Descripción	Prioridad	Criterio de Aceptación
		financieras representan el principal nicho de mercado.		Auditoría Externa y evaluar los sistemas de tecnologías de información.
008	Procedimientos formalizados	Los documentos deben elaborarse de conformidad al estándar aprobado en la firma EEQA. El idioma empleado debe ser el español.	Alta	Aprobación de los socios de la firma y de la Gerencia de Auditoría.
009	Formulación de un Plan de Trabajo para la revisión de la Infraestructura Tecnológica.	Corresponde al producto profesional de auditoría informática, que se pondrá a disposición del mercado nacional e internacional.	Alta	Diseño, oficialización e implementación de un Plan de Trabajo para la revisión de la Infraestructura Tecnológica, que considere los recursos de TI: Información, Infraestructura, Sistemas de Información y Recursos Humanos.

Fuente: (El Autor, 2018)

Los requisitos antes expuestos, permiten delimitar el alcance que posee el proyecto para crear un plan para auditar un sistema de gestión de seguridad de la información. La división del trabajo requerido se representa a través de una EDT (Estructura de Desglose de Trabajo), instrumento que muestra jerárquicamente todas las actividades necesarias para desarrollar el proyecto, desde el levantamiento inicial de los requerimientos, la formulación e implementación del plan de auditoría y finalmente el establecimiento de las tareas correspondientes al cierre del proyecto, todo lo anterior para alcanzar los objetivos propuestos y crear los entregables requeridos.


1. Metodología para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Firma de Consultoría EEQA
1.1 Requisitos del Proyecto
1.1.1 Reunión con la Firma de Consultoría EEQA
1.1.1.1 Levantamiento de Requisitos Generales del Proyecto
1.1.1.2 Levantamiento de Requisitos Técnicos del Proyecto
1.1.2 Seguimiento y Control
1.2 Especificación del Marco Normativo
1.2.1 Legislación Costarricense
1.2.1.1 Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR
1.2.1.2 Acuerdo SUGEF 14-17
1.2.2 Estándares y Marcos de Referencia Internacionales
1.2.2.1 COBIT - ISACA
1.2.2.2 ITIL
1.2.2.3 ISO-27001
1.2.3 Seguimiento y Control


1.3 Implementación de Herramientas Tecnológicas
1.3.1 Herramientas para el Análisis de Datos
1.3.1.1 Análisis de viabilidad para la instalación de la herramienta "ACL"
1.3.1.2 Análisis de viabilidad para la instalación de la herramienta "IDEA"
1.3.1.3 Análisis de viabilidad para la instalación de la herramienta "TOAD"
1.3.2 Herramientas para el Escaneo de Vulnerabilidades
1.3.2.1 Escaneo de Vulnerabilidades de Servidores (Microsoft, UNIX, LINUX)
1.3.2.2 Escaneo de Vulnerabilidades de Redes (CISCO, JUNIPER, HUAWEI)
1.3.2.3 Escaneo de Vulnerabilidades de Bases de Datos (Oracle, SQL Server, MySQL)
1.3.3 Seguimiento y Control
1.4 Elaboración y Formalización de los Lineamientos de Auditoría
1.4.1 Elaboración de Políticas
1.4.2 Elaboración de Procedimientos
1.4.3 Elaboración de Instructivos y Manuales
1.4.4 Seguimiento y Control

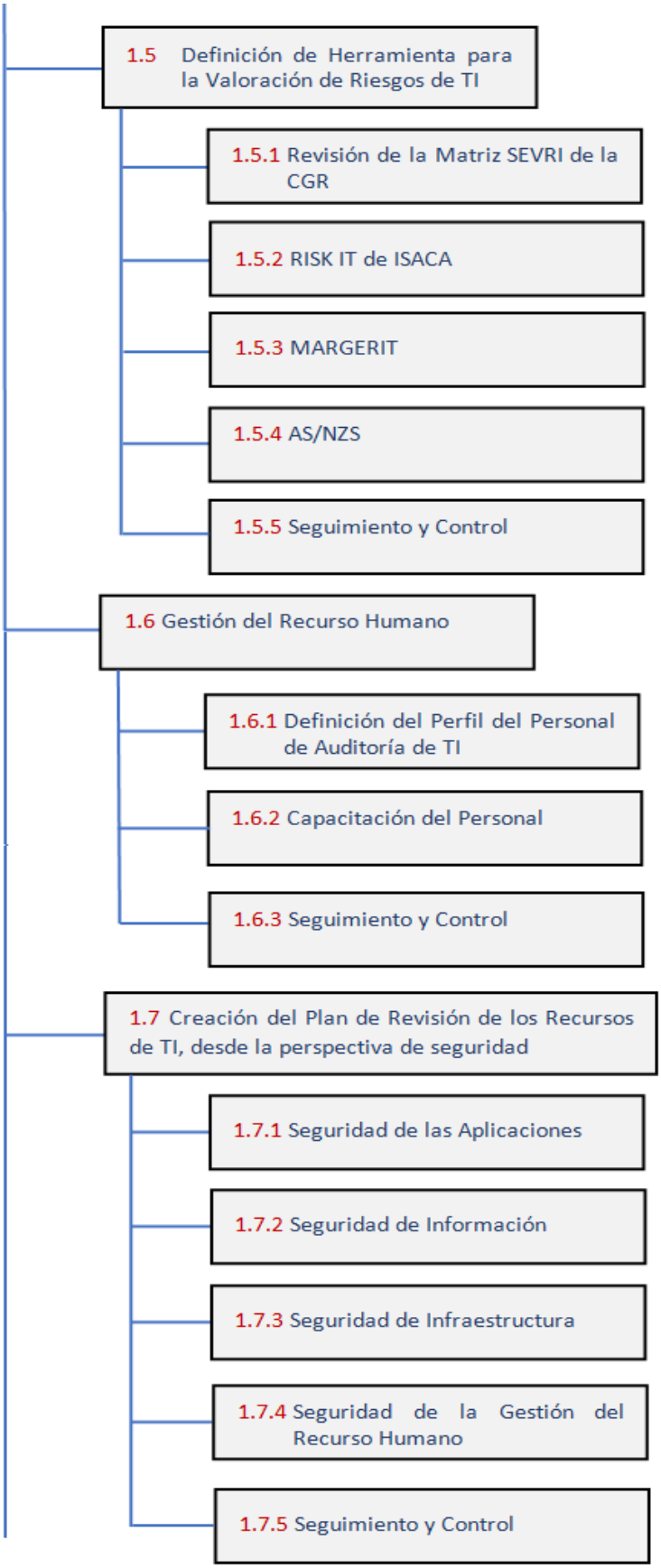

1.5 Definición de Herramienta para la Valoración de Riesgos de TI
1.5.1 Revisión de la Matriz SEVRI de la CGR
1.5.2 RISK IT de ISACA
1.5.3 MARGERIT
1.5.4 AS/NZS
1.5.5 Seguimiento y Control
1.6 Gestión del Recurso Humano
1.6.1 Definición del Perfil del Personal de Auditoría de TI
1.6.2 Capacitación del Personal
1.6.3 Seguimiento y Control
1.7 Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad
1.7.1 Seguridad de las Aplicaciones
1.7.2 Seguridad de Información
1.7.3 Seguridad de Infraestructura
1.7.4 Seguridad de la Gestión del Recurso Humano
1.7.5 Seguimiento y Control

Figura No. 6. Estructura de Desglose de Trabajo del Proyecto
Fuente: (El Autor, 2018)

El detalle de cada uno de los componentes que conforman la Estructura de Desglose de Trabajo del Proyecto anterior, se consigna en los cuadros Nos.12,13,14,15,16,17,18 y 19, especificando de esta forma al equipo humano del proyecto los pormenores de los entregables que deben desarrollarse y la forma óptima para hacerlo.

Cuadro No. 12: Diccionario de la EDT 1.1

ID: 1.1	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Levantamiento de los requisitos del proyecto			
Criterio de Aceptación: Determinar los requerimientos de identificados por el recurso humano que conforma la Firma EEQA			

<table>
<tr><td colspan="4">Entregables: Documento con la totalidad de los requisitos del proyecto.</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 3 días</td></tr>
<tr><td colspan="4">Hitos: 20-02-2018 Levantamiento de requisitos generales del proyecto
21-02-2018 Levantamiento de requisitos técnicos del proyecto</td></tr>
<tr><td colspan="4">Costo: $ 3.225</td></tr>
<tr><td>ID: 1.1.1</td><td>Cuenta Control: 1.1</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Director del Proyecto</td></tr>
<tr><td colspan="4">Descripción: Reunión con los miembros de la Firma EEQA</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Debidamente firmado por todos los asistentes a la reunión, como evidencia de la aceptación de los puntos tratados.</td></tr>
<tr><td colspan="4">Entregables: Minuta de los acuerdos tomados por el equipo del proyecto</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 3 días</td></tr>
<tr><td colspan="4">Hitos: 20-02-2018 Levantamiento de requisitos generales del proyecto
21-02-2018 Levantamiento de requisitos técnicos del proyecto</td></tr>
<tr><td colspan="4">Costo: $ 1381</td></tr>
<tr><td>ID: 1.1.1.1</td><td>Cuenta Control: 1.1</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Director del Proyecto</td></tr>
<tr><td colspan="4">Descripción: Levantamiento de requisitos generales del proyecto</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Determinar los requerimientos de identificados por el recurso humano que conforma la Firma EEQA</td></tr>
<tr><td colspan="4">Entregables: Documento con los requisitos generales del proyecto</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 2 días</td></tr>
</table>

Hitos: 20-02-2018 Levantamiento de requisitos generales del proyecto			
Costo: $ 922			
ID: 1.1.1.2	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Levantamiento de requisitos técnicos del proyecto			
Criterio de Aceptación: Determinar los requerimientos de índole técnico establecidos por el recurso humano de la Firma EEQA			
Entregables: Documento con los requisitos técnicos del proyecto			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 21-02-2018 Levantamiento de requisitos técnicos del proyecto			
Costo: $ 922			
ID: 1.1.2	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			
Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.			
Entregables: Informe de seguimiento del avance del proyecto			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 26-02-2018 Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo Aplicable			
Costo: $ 622			

Fuente: (El Autor, 2018)

Cuadro No. 13: Diccionario de la EDT 1.2

ID: 1.2	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Especificación del Marco Normativo			
Criterio de Aceptación:			
Entregables: Documento que detalla el Marco Normativo aplicable en el desarrollo del plan de auditoría del SGSI			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 3 días			
Hitos: 23-02-2018 Legislación Costarricense 26-02-2018 Estándares y Marcos de Referencia Internacionales			
Costo: $ 1.938			
ID: 1.2.1	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Análisis de la Legislación Costarricense			
Criterio de Aceptación: Identificar los aspectos requeridos para el cumplimiento de los lineamientos dados por la Contraloría General de la República.			
Entregables: Documento que detalla el Marco Normativo de Costa Rica que es aplicable en el desarrollo del plan de auditoría del SGSI			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre el cumplimiento de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR 23-02-2018 Informe sobre el cumplimiento del acuerdo SUGEF 14-17			

Costo: $ 188 cada uno de los Hitos supracitados.			
ID: 1.2.1.1	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR.			
Criterio de Aceptación: Identificar los aspectos requeridos para el cumplimiento de los lineamientos dados por la Contraloría General de la República.			
Entregables: Evaluación de las implicaciones de elaborar un plan de auditoría de conformidad con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre el cumplimiento de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR			
Costo: $ 188			
ID: 1.2.1.2	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión del acuerdo SUGEF 14-17			
Criterio de Aceptación: Identificar los aspectos necesarios para el cumplimiento de las directrices giradas por la SUGEF.			
Entregables: Evaluación de las implicaciones de elaborar un plan de auditoría de conformidad con el acuerdo SUGEF 14-17.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre el cumplimiento del acuerdo SUGEF 14-17			
Costo: $ 188			

ID: 1.2.2	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Análisis de los estándares y marcos de referencia internacionales			
Criterio de Aceptación: Delimitación de los procesos, objetivos de control y estándares entre otros, que son aplicables en Costa Rica.			
Entregables: Informes de viabilidad de implementar estándares y marcos de referencia internacionales.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 3 días			
Hitos: 23-02-2018 Informe sobre la viabilidad de la aplicación del marco de referencia COBIT 5 23-02-2018 Informe sobre la viabilidad de la aplicación de la metodología ITIL v3 23-02-2018 Informe sobre la viabilidad de la aplicación del estándar ISO-27001			
Costo: $ 188 cada uno de los Hitos supracitados.			
ID: 1.2.2.1	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión del marco de referencia COBIT 5			
Criterio de Aceptación: Establecer los recursos necesarios para evaluar objetivamente el nivel de madurez de la gestión de TI, a través de COBIT.			
Entregables: Informe sobre la viabilidad de la aplicación del marco de referencia COBIT 5			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre la viabilidad de la aplicación del marco de referencia COBIT 5			
Costo: $ 188			

ID: 1.2.2.2	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión de la metodología ITIL v3			
Criterio de Aceptación: Establecer los recursos requeridos para la evaluación del diseño y la prestación de los servicios de TI, mediante ITIL.			
Entregables: Informe sobre la viabilidad de la aplicación de la metodología ITIL v3			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre la viabilidad de la aplicación de la metodología ITIL v3			
Costo: $ 188			
ID: 1.2.2.3	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión del estándar ISO-27001			
Criterio de Aceptación: Establecer los recursos necesarios para evaluar el Sistema de Gestión de Seguridad de la Información, de conformidad con ISO-27001.			
Entregables: Informe sobre la viabilidad de la aplicación del estándar ISO-27001			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-02-2018 Informe sobre la viabilidad de la aplicación del estándar ISO-27001			
Costo: $ 188			
ID: 1.2.3	Cuenta Control: 1.2	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			

Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.
Entregables: Informe de seguimiento del avance del proyecto
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.
Duración: 1 día
Hitos: 26-02-2018 Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo Aplicable
Costo: $ 622

Fuente: (El Autor, 2018)

Cuadro No. 14: Diccionario de la EDT 1.3

ID: 1.3	Cuenta Control: 1.3	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Implementación de herramientas tecnológicas			
Criterio de Aceptación: Alineamiento con los requerimientos técnicos establecidos y con el presupuesto accionado para la adquisición.			
Entregables: Análisis de viabilidad para la instalación de las herramientas tecnológicas.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 14 días Debido a la complejidad de las actividades, se establece una “Reserva por Contingencia” de 4 días.			
Hitos: 05-03-2018 Herramientas para el Análisis de Datos 16-03-2018 Herramientas para el Escaneo de Vulnerabilidades			

<table>
<tr><td colspan="4">Costo: $ 5.406</td></tr>
<tr><td>ID: 1.3.1</td><td>Cuenta Control: 1.3</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Equipo de Auditores</td></tr>
<tr><td colspan="4">Descripción: Herramientas para el análisis de datos</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Alineamiento con los requerimientos técnicos establecidos y con el presupuesto accionado para la adquisición.</td></tr>
<tr><td colspan="4">Entregables: Análisis de viabilidad para la instalación de las herramientas tecnológicas.</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 5 días</td></tr>
<tr><td colspan="4">Hitos: 05-03-2018 Informe sobre la viabilidad de la implementación de “ACL”
05-03-2018 Informe sobre la viabilidad de la implementación de “IDEA”
05-03-2018 Informe sobre la viabilidad de la implementación de “TOAD”</td></tr>
<tr><td colspan="4">Costo: $ 598 cada uno de los Hitos supracitados</td></tr>
<tr><td>ID: 1.3.1.1</td><td>Cuenta Control: 1.1</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Equipo de Auditores</td></tr>
<tr><td colspan="4">Descripción: Análisis de viabilidad para la instalación de la herramienta “ACL”</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Determinar el alcance de la herramienta “ACL” y establecer los elementos necesarios para su incorporación en la firma EEQA.</td></tr>
<tr><td colspan="4">Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 5 días</td></tr>
<tr><td colspan="4">Hitos: 05-03-2018 Informe sobre la viabilidad de la implementación de “ACL”</td></tr>
</table>

Costo: $ 598			
ID: 1.3.1.2	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Análisis de viabilidad para la instalación de la herramienta “IDEA”			
Criterio de Aceptación: Determinar el alcance de la herramienta “IDEA” y establecer los elementos necesarios para su incorporación en la Firma EEQA.			
Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 05-03-2018 Informe sobre la viabilidad de la implementación de “IDEA”			
Costo: $ 598			
ID: 1.3.1.3	Cuenta Control: 1.1	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Análisis de viabilidad para la instalación de la herramienta “TOAD”			
Criterio de Aceptación: Determinar el alcance de la herramienta “TOAD” y establecer los elementos necesarios para su incorporación en la Firma EEQA.			
Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 05-03-2018 Informe sobre la viabilidad de la implementación de “TOAD”			
Costo: $ 598			

ID: 1.3.2	Cuenta Control: 1.3	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Herramientas para el escaneo de vulnerabilidades			
Criterio de Aceptación: Alineamiento con los requerimientos técnicos establecidos y con el presupuesto accionado para la adquisición.			
Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 09-03-2018 Informe de la herramienta para escaneo de vulnerabilidades en Servidores 09-03-2018 Informe de la herramienta para escaneo de vulnerabilidades en Redes 09-03-2018 Informe de la herramienta para escaneo de las Bases de Datos			
Costo: $ 598 cada uno de los Hitos supracitados			
ID: 1.3.2.1	Cuenta Control: 1.3	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Escaneo de vulnerabilidades de servidores			
Criterio de Aceptación: Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “MBSA”, “Kali Linux” y “REMnux”.			
Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			

<table>
<tr><td colspan="4">Hitos: 09-03-2018 Informe de la herramienta para escaneo de vulnerabilidades en Servidores</td></tr>
<tr><td colspan="4">Costo: $ 598</td></tr>
<tr><td>ID: 1.3.2.2</td><td>Cuenta Control: 1.3</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Asesor Tecnológico</td></tr>
<tr><td colspan="4">Descripción: Escaneo de vulnerabilidades de equipos de telecomunicaciones</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “GFI Languard”, “Wireshark”, “OpUtils” y “ForeScout”.</td></tr>
<tr><td colspan="4">Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 5 días</td></tr>
<tr><td colspan="4">Hitos: 09-03-2018 Informe de la herramienta para escaneo de vulnerabilidades en Redes</td></tr>
<tr><td colspan="4">Costo: $ 598</td></tr>
<tr><td>ID: 1.3.2.3</td><td>Cuenta Control: 1.3</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Asesor Tecnológico</td></tr>
<tr><td colspan="4">Descripción: Escaneo de vulnerabilidades de bases de datos</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “Advanced SQL Password Recovery”, “QualysGuard” y “SQLPing3”; asimismo, desarrollar scripts propios para la revisión de las Bases de Datos.</td></tr>
<tr><td colspan="4">Entregables: Análisis de viabilidad que incluya el tipo de licencia requerida, capacitación, costo, requerimientos técnicos, referencias, representante en Costa Rica del software.</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de</td></tr>
</table>

Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 09-03-2018 Informe de la herramienta para escaneo de las Bases de Datos			
Costo: $ 598			
ID: 1.3.3	Cuenta Control: 1.3	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			
Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.			
Entregables: Informe de seguimiento del avance del proyecto			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 12-03-2018 Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Implementar			
Costo: $ 622			

Fuente: (El Autor, 2018)

Cuadro No. 15: Diccionario de la EDT 1.4

ID: 1.4	Cuenta Control: 1.4	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Elaboración y formalización de los lineamientos de auditoría de TI			
Criterio de Aceptación: Alineadas con el directrices emitidas con anterioridad por la Firma EEQA, que norman su función consultora.			
Entregables: Establecimiento del marco de control Interno para la planificación y			

<table>
<tr><td colspan="4">ejecución de la auditoría del SGSI.</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de Talento Humano.</td></tr>
<tr><td colspan="4">Duración: 17 días</td></tr>
<tr><td colspan="4">Hitos: 23-03-2018 Elaboración de Políticas
06-04-2018 Elaboración de Procedimientos
12-04-2018 Elaboración de Instructivos y Manuales</td></tr>
<tr><td colspan="4">Costo: $ 5.662</td></tr>
<tr><td>ID: 1.4.1</td><td>Cuenta Control: 1.4</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Equipo de Auditores</td></tr>
<tr><td colspan="4">Descripción: Elaboración de políticas</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Diseño, oficialización e implementación de las políticas.</td></tr>
<tr><td colspan="4">Entregables: Políticas de Auditoría de TI</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de Talento Humano.</td></tr>
<tr><td colspan="4">Duración: 5 días</td></tr>
<tr><td colspan="4">Hitos: 23-03-2018 Elaboración de Políticas</td></tr>
<tr><td colspan="4">Costo: $ 1.200</td></tr>
<tr><td>ID: 1.4.2</td><td>Cuenta Control: 1.4</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Equipo de Auditores</td></tr>
<tr><td colspan="4">Descripción: Elaboración de procedimientos</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Diseño, oficialización e implementación de los procedimientos.</td></tr>
<tr><td colspan="4">Entregables: Procedimientos de Auditoría de TI</td></tr>
<tr><td colspan="4">Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de</td></tr>
</table>

Talento Humano.			
Duración: 8 días			
Hitos: 06-04-2018 Elaboración de Procedimientos			
Costo: $ 3.120			
ID: 1.4.3	Cuenta Control: 1.4	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Elaboración de instructivos y manuales			
Criterio de Aceptación: Diseño, oficialización e implementación de los manuales e instructivos.			
Entregables: Instructivos y Manuales de Auditoría de TI			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de Talento Humano. Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de Talento Humano.			
Duración: 3 días			
Hitos: 12-04-2018 Elaboración de Instructivos y Manuales			
Costo: $ 720			
ID: 1.4.4	Cuenta Control: 1.4	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			
Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.			
Entregables: Informe de seguimiento del avance del proyecto			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores, Asesor Tecnológico y Encargada de Gestión de Talento Humano.			

Duración: 1 día
Hitos: 13-04-2018 Punto de Control No.3: Evaluación de los Procedimientos de Auditoría
Costo: $ 622

Fuente: (El Autor, 2018)

Cuadro No. 16: Diccionario de la EDT 1.5

ID: 1.5	Cuenta Control: 1.5	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Definición de la herramienta para la valoración de riesgos de TI			
Criterio de Aceptación: Actualización de la matriz de conformidad con los riesgos vinculados a la gestión de TI.			
Entregables: Informe sobre herramienta para la valoración de riesgos de TI seleccionada.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 17-04-2018 Matriz SEVRI de la Contraloría General de la República 18-04-2018 Valoración de RISK IT 19-04-2018 Valoración de MARGERIT 20-04-2018 Valoración de AS/NZS			
Costo: **$ 2.232**			
ID: 1.5.1	Cuenta Control: 1.5	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión de la matriz SEVRI de la CGR			
Criterio de Aceptación: Incorporar la aplicación de la Matriz SEVRI, como parte del			

plan de auditoría a desarrollar.			
Entregables: Actualización de la matriz de conformidad con los riesgos vinculados a la gestión de TI.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 17-04-2018 Matriz SEVRI de la Contraloría General de la República			
Costo: $ 446			
ID: 1.5.2	Cuenta Control: 1.5	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión de la herramienta RISK IT de ISACA			
Criterio de Aceptación: Determinar el alcance de la metodología “RISK IT” y valorar los elementos necesarios para su aplicación en la firma EEQA.			
Entregables: Estudio de la metodología “RISK IT” de ISACA.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 18-04-2018 Valoración de RISK IT			
Costo: $ 894			
ID: 1.5.3	Cuenta Control: 1.5	Última Actualización: 13-06-2018	Responsable: Equipo de Auditores
Descripción: Revisión de la metodología MARGERIT			
Criterio de Aceptación: Determinar el alcance del marco de referencia “MARGERIT” y valorar los puntos necesarios para su utilización en la Firma EEQA.			
Entregables: Estudio del marco de referencia “MARGERIT”.			
Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.			

<table>
<tr><td colspan="4">Duración:1 día</td></tr>
<tr><td colspan="4">Hitos: 19-04-2018 Valoración de MARGERIT</td></tr>
<tr><td colspan="4">Costo: $ 446</td></tr>
<tr><td>ID: 1.5.4</td><td>Cuenta Control: 1.5</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Equipo de Auditores</td></tr>
<tr><td colspan="4">Descripción: Revisión de la Norma AS/NZS</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Determinar el alcance de la Norma “AS/NZS” y evaluar los aspectos necesarios para su aplicación en la Firma EEQA.</td></tr>
<tr><td colspan="4">Entregables: Estudio de la Norma “AS/NZS”.</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 1 día</td></tr>
<tr><td colspan="4">Hitos: 20-04-2018 Valoración de AS/NZS</td></tr>
<tr><td colspan="4">Costo: $ 446</td></tr>
<tr><td>ID: 1.5.5</td><td>Cuenta Control: 1.5</td><td>Última Actualización: 13-06-2018</td><td>Responsable: Director del Proyecto</td></tr>
<tr><td colspan="4">Descripción: Seguimiento y Control</td></tr>
<tr><td colspan="4">Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.</td></tr>
<tr><td colspan="4">Entregables: Informe de seguimiento del avance del proyecto</td></tr>
<tr><td colspan="4">Recursos Asignados: Director del Proyecto, Gerente de Auditoría, Equipo de Auditores y Asesor Tecnológico.</td></tr>
<tr><td colspan="4">Duración: 1 día</td></tr>
<tr><td colspan="4">Hitos: 16-04-2018 Reunión de seguimiento sobre el avance del proyecto</td></tr>
<tr><td colspan="4">Costo: Al tratarse de una reunión rápida de seguimiento de no más de 20 minutos, el costo de la actividad se distribuye entre las 4 actividades que conforman el punto 1.5 y cuyo costo es $ 2.232.</td></tr>
</table>

Fuente: (El Autor, 2018)

Cuadro No. 17: Diccionario de la EDT 1.6

ID: 1.6	Cuenta Control: 1.6	Última Actualización: 13-06-2018	Responsable: Encargada de Gestión de Talento Humano
Descripción: Gestión del Recurso Humano			
Criterio de Aceptación: Establecimientos de las competencias requeridas por el personal de la Firma EEQA, que va a desarrollar la auditoría del SGSI.			
Entregables: Definición del Perfil del personal de Auditoría de TI y su correspondiente plan de capacitación.			
Recursos Asignados: Gerente de Auditoría, Director del Proyecto, Encargada de Gestión de Talento Humano y Asesor Tecnológico.			
Duración: 2 días			
Hitos: 23-04-2018 Definición del perfil del personal de auditoría de TI 24-04-2018 Presentación del plan de capacitación del personal de la Firma EEQA.			
Costo: **$ 1.244**			
ID: 1.6.1	Cuenta Control: 1.6	Última Actualización: 13-06-2018	Responsable: Encargada de Gestión de Talento Humano
Descripción: Definición del perfil del personal de auditoría de TI			
Criterio de Aceptación: Definir la modalidad de contratación, ya sea por servicios profesionales o contratación por tiempo indefinido.			
Entregables: Requisitos del personal que ejecutará la auditoría del Sistema de Gestión de Seguridad de la Información.			
Recursos Asignados: Gerente de Auditoría, Director del Proyecto, Encargada de Gestión de Talento Humano y Asesor Tecnológico.			

Duración: 1 día			
Hitos: 23-04-2018 Definición del perfil del personal de auditoría de TI			
Costo: $ 622			
ID: 1.6.2	Cuenta Control: 1.6	Última Actualización: 13-06-2018	Responsable: Encargada de Gestión de Talento Humano
Descripción: Capacitación del personal de auditoría de TI			
Criterio de Aceptación: Proporcionar al personal de la Firma EEQA los conocimientos y habilidades necesarias para la ejecución de sus funciones y asumir sus responsabilidades.			
Entregables: Plan de capacitación del personal de la firma EEQA.			
Recursos Asignados: Gerente de Auditoría, Director del Proyecto, Encargada de Gestión de Talento Humano y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 24-04-2018 Presentación del plan de capacitación del personal de la Firma EEQA.			
Costo: $ 622			
ID: 1.6.3	Cuenta Control: 1.6	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			
Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.			
Entregables: Informe de seguimiento del avance del proyecto			
Recursos Asignados: Gerente de Auditoría, Director del Proyecto, Encargada de Gestión de Talento Humano y Asesor Tecnológico.			
Duración: 1 día			
Hitos: 23-04-2018 Reunión de seguimiento sobre el avance del proyecto			

Costo: Al tratarse de una reunión rápida de seguimiento de no más de 20 minutos, el costo de la actividad se distribuye entre las 2 actividades que conforman el punto 1.6 y cuyo costo es **$ 1.244**.

Fuente: (El Autor, 2018)

Cuadro No. 18: Diccionario de la EDT 1.7

ID: 1.7	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Creación del plan de revisión de los recursos de TI, desde la perspectiva de seguridad			
Criterio de Aceptación: El Plan de Auditoría debe enfatizar en la evaluación de la razonabilidad del Sistema de Gestión de Seguridad de la Información (SGSI).			
Entregables: Planes para la revisión de los recursos de TI (Infraestructura, aplicaciones, recursos humano e información).			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 26 días Debido a la complejidad de las actividades, se establece una “Reserva por Contingencia” de 5 días.			
Hitos: 31-05-2018 Creación del Plan de Revisión de los Recursos de TI desde la perspectiva de Seguridad			
Costo: $ 6.646			
ID: 1.7.1	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Seguridad de las aplicaciones			

Criterio de Aceptación: Establecimiento de las distintas actividades a desarrollar por el equipo de profesionales de la Firma EEQA, para asegurar la correcta gestión de los riesgos vinculados a las aplicaciones y su acceso, principalmente desde Internet.			
Entregables: Plan para la revisión de aplicaciones, desde la perspectiva de seguridad.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 02-05-2018 Plan para evaluar la seguridad de las aplicaciones			
Costo: $ 1,506			
ID: 1.7.2	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Seguridad de la información			
Criterio de Aceptación: Definición de las distintas actividades a desarrollar por el equipo de profesionales de la Firma EEQA, para asegurar la integridad, confidencialidad y disponibilidad de la información de sus clientes.			
Entregables: Plan para la revisión de la seguridad de la información.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 4 días			
Hitos: 08-05-2018 Plan para evaluar la seguridad de la información			
Costo: $ 1,506			
ID: 1.7.3	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Seguridad de infraestructura			
Criterio de Aceptación: Establecimiento de las distintas actividades a ejecutar por			

el equipo de profesionales de la Firma EEQA, para verificar la seguridad y alta disponibilidad de la Infraestructura Tecnológica de sus clientes, considerando para ello las barreras físicas y los mecanismos lógicos de control.			
Entregables: Plan para la revisión de infraestructura de TI, desde la perspectiva de seguridad.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 15-05-2018 Plan para evaluar la seguridad de la infraestructura			
Costo: $ 1,506			
ID: 1.7.4	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Asesor Tecnológico
Descripción: Seguridad de la gestión del recurso humano			
Criterio de Aceptación: Validar la existencia de planes para disminuir la dependencia sobre personal de TI, planes de sucesión del personal, traspaso del conocimiento y segregación de funciones, entre otros aspectos.			
Entregables: Plan para el seguimiento de la función del recurso humano de TI, desde la perspectiva de seguridad.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.			
Duración: 5 días			
Hitos: 23-05-2018 Plan para evaluar la seguridad de la gestión del recurso humano			
Costo: $ 1,506			
ID: 1.7.5	Cuenta Control: 1.7	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Seguimiento y Control			
Criterio de Aceptación: Identificar preventivamente, desviaciones del plan original			

del proyecto; asimismo, corregir errores o defectos en los entregables del proyecto.
Entregables: Informe de seguimiento del avance del proyecto
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma y Asesor Tecnológico.
Duración: 1 día
Hitos: 31-05-2018 Punto de Control No.4: Evaluación del Plan para la Revisión del SGSI
Costo: $ 622

Fuente: (El Autor, 2018)

Cuadro No. 19: Diccionario de la EDT 1.8

ID: 1.8	Cuenta Control: 1.8	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Entrega del proyecto			
Criterio de Aceptación: Firma de aceptación del entregable			
Entregables: Acta de entrega del proyecto.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría y Equipo de Auditores de la Firma.			
Duración: 3 días			
Hitos: 06-06-2018 Entrega del proyecto			
Costo: $ 425			
ID: 1.8.1	Cuenta Control: 1.8	Última Actualización: 13-06-2018	Responsable: Director del Proyecto

Descripción: Firma de aceptación de los entregables del proyecto			
Criterio de Aceptación: Formalización de los entregables del proyecto y visto bueno de parte de la Firma EEQA.			
Entregables: Acta de entrega del proyecto.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría y Equipo de Auditores de la Firma.			
Duración: 1 día			
Hitos: 04-06-2018 Firma de aceptación de los entregables del proyecto			
Costo: $ 85			
ID: 1.8.2	Cuenta Control: 1.8	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Facturación del proyecto			
Criterio de Aceptación: Implica la facturación final del proyecto, debido principalmente a la contratación de una asesoría en el tema de Seguridad Informática.			
Entregables: Pago de la asesoría técnica del proyecto.			
Recursos Asignados:			
Duración: 1 día			
Hitos: 04-06-2018 Facturación del proyecto			
Costo: $ 85			
ID: 1.8.3	Cuenta Control: 1.8	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Documentación del proyecto			
Criterio de Aceptación: Completar la documentación del proyecto acorde con los lineamientos establecidos por la Firma EEQA.			
Entregables: Expediente del proyecto			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría y Equipo de Auditores de la Firma.			

Duración: 1 día			
Hitos: 05-06-2018 Documentación general del proyecto			
Costo: $ 85			
ID: 1.8.3.1	Cuenta Control: 1.8.3	Última Actualización: 13-06-2018	Responsable:
Descripción: Documentación de las lecciones aprendidas del proyecto			
Criterio de Aceptación: Incluye la información sobre las desviaciones presentadas en el proyecto y las acciones correctivas aplicadas.			
Entregables: Documentación de las Lecciones Aprendidas			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría y Equipo de Auditores de la Firma.			
Duración: 1 día			
Hitos: 05-06-2018 Documentación de las Lecciones Aprendidas			
Costo: $ 85			
ID: 1.8.4	Cuenta Control: 1.8	Última Actualización: 13-06-2018	Responsable: Director del Proyecto
Descripción: Cierre de Adquisiciones			
Criterio de Aceptación: Se documentan los acuerdos relacionados con las adquisiciones del proyecto.			
Entregables: Plan de gestión de las adquisiciones.			
Recursos Asignados: Socios de la Firma, Director del Proyecto, Gerente de Auditoría y Equipo de Auditores de la Firma.			
Duración: 1 día			
Hitos: 06-06-2018 Informe del cierre de las adquisiciones del proyecto			
Costo: $ 85			

Fuente: (El Autor, 2018)

Con el objetivo de llevar el registro de los requisitos del proyecto, así como de los entregables que posibilitan su debido cumplimiento, se desarrolla la siguiente matriz de trazabilidad:

Cuadro No. 20: Matriz de Trazabilidad de los Requisitos

ID	Prioridad	Responsable	Categoría	Descripción del Requerimiento	EDT
001	Alta	Socios de la Firma Gerente de Auditoría	Alcance del Producto	**Alineación con las buenas prácticas y marcos de referencia de TI:** La auditoría a desarrollar debe permitir evaluar el grado de madurez en la aplicación de buenas prácticas por medio del marco de referencia de los Objetivos de Control de COBIT y la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL).	1.2
002	Alta	Gerente de Auditoría Equipo de Auditores de la Firma	Alcance del Producto	**Flexibilidad de aplicación independietemente del segmento de negocios al que pertenece el cliente:** No debe exitir limitaciones en la aplicación del plan de auditoría a desarrollar. El	1.1

ID	Prioridad	Responsable	Categoría	Descripción del Requerimiento	EDT
				mismo podrá ser ejecutado en organizaciones sin importantar su dimensión o su giro de negocios.	
003	Alta	Socios de la Firma Gerente de Auditoría Asesor experto en Seguridad Informática	Alcance del Producto	**Incorporación de herramientas tecnológicas:** La auditoría a implementar debe permitir la incorporación de herramientas tecnológicas que suministren mayor profundidad a la revisión, así como la automatización de tareas.	1.3
004	Alta	Gerente de Auditoría Equipo de Auditores de la Firma EEQA	Alcance del Producto	**Instrumento para la valoración de riesgos:** Se debe incorporar como parte del plan de auditoría, un instrumento para la evaluación cualitativa y cuantitativa del riesgo vinculado con la gestión de las tecnologías de información.	1.5
005	Alta	Gerente de Auditoría Encargada del Área	Alcance del Proyecto	**Capacitar al personal de auditoría en temas relacionados con las tecnologías de**	1.6

ID	Prioridad	Responsable	Categoría	Descripción del Requerimiento	EDT
		de Gestión de Talento Humano		**información:** Entre las capacitaciones propuestas, se encuentran COBIT 5, ISO 27001 e ITIL v3. Estos marcos permiten el desarrollo del enfoque de supervisión basado en riesgos.	
006	Media	Gerente de Auditoría Equipo de Auditores de la Firma EEQA	Alcance del Proyecto	**Obtención de certificaciones de seguridad informática y de gestión de TI:** La industria y los profesionales en TI, han desarrollado estándares y marcos que permiten gestionar y controlar las tecnologías. La obtención de certificaciones internacionales tiene repercusión en la reputación de la firma.	1.2
007	Alta	Gerente de Auditoría	Alcance del Proyecto	**Evaluación de la Norma 14-17 SUGEF:** Formar parte del Registro de Auditores elegibles de la	1.2

ID	Prioridad	Responsable	Categoría	Descripción del Requerimiento	EDT
				SUGEF. De esta forma, la Firma EEQA se encontrará habilitada para participar como Auditoría Externa y evaluar los sistemas de tecnologías de información.	
008	Alta	Socios de la Firma. Gerente de Auditoría Encargada del área de Gestión de Talento Humano	Alcance del Producto	**Procedimientos formalizados:** Los documentos deben elaborarse de conformidad al estándar aprobado en la Firma EEQA. El idioma empleado debe ser el español.	1.4
009	Alta	Socios de la Firma Gerente de Auditoría Equipo de Auditores de la Firma EEQA Asesor experto en Seguridad Informática	Alcance del Producto	**Formulación de un Plan de Trabajo para la revisión de la Infraestructura Tecnológica:** Corresponde al producto profesional de auditoría informática, que se pondrá a disposición del mercado nacional e internacional.	1.7

Fuente: (El Autor, 2018)

4.3 Plan de Gestión del Cronograma

La gestión del tiempo consigna los procesos necesarios para gestionar la terminación del proyecto de conformidad con el plazo determinado. Para ello, se inicia con el Plan de Gestión del Cronograma, a través del cual se establecen todas las actividades del cronograma necesarias para el desarrollo del proyecto; asimismo, se incluye un identificador de la actividad, el paquete del trabajo del cual forma parte y una descripción del alcance del trabajo requerido acorde con la Estructura de Desglose de Trabajo supracitada. Dicha información se representa en el cuadro adjunto:

Cuadro No. 21: Lista de Actividades del Proyecto

Actividad	Paquete de Trabajo	Entregable	Descripción
1.1 Requisitos del Proyecto	1.1.1 Reunión con la Firma de Consultoría EEQA	1.1.1.1 Levantamiento de Requisitos Generales del Proyecto	Determinar los requerimientos de identificados por el recurso humano que conforma la Firma EEQA
		1.1.1.2 Levantamiento de Requisitos Técnicos del Proyecto	Determinar los requerimientos de índole técnico establecidos por el recurso humano de la Firma EEQA
	1.1.2 Seguimiento y Control	1.1.2.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.
1.2	1.2.1	1.2.1.1 Normas	Identificar los aspectos

Actividad	Paquete de Trabajo	Entregable	Descripción
Especificación del Marco Normativo	Legislación Costarricense	Técnicas para la Gestión y el Control de las TI, emitidas por la CGR	requeridos para el cumplimiento de los lineamientos dados por la Contraloría General de la República.
		1.2.1.2 Acuerdo SUGEF 14-17	Identificar los aspectos necesarios para el cumplimiento de las directrices giradas por la SUGEF.
	1.2.2 Estándares y Marcos de Referencia Internacionales	1.2.2.1 Informe sobre COBIT - ISACA	Establecer los recursos necesarios para evaluar objetivamente el nivel de madurez de la gestión de TI, a través de COBIT.
		1.2.2.2 Informe sobre ITIL	Establecer los recursos requeridos para la evaluación del diseño y la prestación de los servicios de TI, mediante ITIL.
		1.2.2.3 Informe sobre ISO-27001	Establecer los recursos necesarios para evaluar el Sistema de Gestión de Seguridad de la Información, de conformidad con ISO-27001.
	1.2.3	1.2.3.1 Informe	Identificar y aplicar las

Actividad	Paquete de Trabajo	Entregable	Descripción
	Seguimiento y Control	de Control y Seguimiento del Proyecto	medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.
1.3 Implementación de Herramientas Tecnológicas	1.3.1 Herramientas para el Análisis de Datos	1.3.1.1 Análisis de viabilidad para la instalación de la herramienta “ACL”	Determinar el alcance de la herramienta “ACL” y establecer los elementos necesarios para su incorporación en la firma EEQA.
		1.3.1.2 Análisis de viabilidad para la instalación de la herramienta “IDEA”	Determinar el alcance de la herramienta “IDEA” y establecer los elementos necesarios para su incorporación en la Firma EEQA.
		1.3.1.3 Análisis de viabilidad para la instalación de la herramienta “TOAD”	Determinar el alcance de la herramienta “TOAD” y establecer los elementos necesarios para su incorporación en la Firma EEQA.
	1.3.2 Herramientas para el Escaneo de Vulnerabilidades	1.3.2.1 Informe sobre escaneo de Vulnerabilidades de Servidores (Microsoft, UNIX, LINUX)	Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “MBSA”, “Kali

Actividad	Paquete de Trabajo	Entregable	Descripción
			Linux” y “REMnux”.
		1.3.2.2 Informe sobre escaneo de Vulnerabilidades de Redes (CISCO, JUNIPER, HUAWEI)	Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “GFI Languard”, “Wireshark”, “OpUtils” y “ForeScout”.
		1.3.2.3 Informe sobre escaneo de vulnerabilidades de Bases de Datos (Oracle, SQL Server, MySQL)	Valorar la implementación de herramientas tanto licenciadas como Open Source, para el escaneo de vulnerabilidades, entre ellas “Advanced SQL Password Recovery”, “QualysGuard” y “SQLPing3”; asimismo, desarrollar scripts propios para la revisión de las Bases de Datos.
	1.3.3 Seguimiento y Control	1.3.3.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.

Actividad	Paquete de Trabajo	Entregable	Descripción
1.4 Elaboración y Formalización de Lineamientos de Auditoría	1.4.1 Elaboración de Políticas.	1.4.1.1 Políticas de Auditoría de TI	Diseño, oficialización e implementación de las políticas.
	1.4.2 Elaboración de Procedimientos	1.4.2.1 Procedimientos de Auditoría de TI	Diseño, oficialización e implementación de los procedimientos.
	1.4.3 Elaboración de Instructivos y Manuales.	1.4.3.1 Instructivos y Manuales de Auditoría de TI	Diseño, oficialización e implementación de los manuales e instructivos.
	1.4.4 Seguimiento y Control	1.4.4.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.
1.5 Definición de Herramienta para la Valoración de Riesgos de TI	1.5.1 Revisión de la Matriz SEVRI de la Contraloría General de la República.	1.5.1.1 Actualización de la matriz de conformidad con los riesgos vinculados a la gestión de TI.	Incorporar la aplicación de la Matriz SEVRI, como parte del plan de auditoría a desarrollar.
	1.5.2 Revisión de la metodología “RISK IT” de ISACA.	1.5.2.1 Estudio de la metodología “RISK IT” de ISACA.	Determinar el alcance de la metodología “RISK IT” y valorar los elementos necesarios para su aplicación en la firma EEQA.

Actividad	Paquete de Trabajo	Entregable	Descripción
	1.5.3 Revisión del marco de referencia “MARGERIT	1.5.3.1 Estudio del marco de referencia “MARGERIT”.	Determinar el alcance del marco de referencia “MARGERIT” y valorar los puntos necesarios para su utilización en la Firma EEQA.
	1.5.4 Revisión de la Norma “AS/NZS”.	1.5.4.1 Estudio de la Norma “AS/NZS”.	Determinar el alcance de la Norma “AS/NZS” y evaluar los aspectos necesarios para su aplicación en la Firma EEQA.
	1.5.5 Seguimiento y Control	1.5.5.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.
1.6 Gestión del Recurso Humano.	1.6.1 Definición del Perfil del personal de Auditoría de TI.	1.6.1.1 Requisitos del personal que ejecutará la auditoría del Sistema de Gestión de Seguridad de la Información.	Definir la modalidad de contratación, ya sea por servicios profesionales o contratación por tiempo indefinido.
	1.6.2 Capacitación del Personal.	1.6.2.1 Plan de capacitación del personal de la	Proporcionar al personal de la Firma EEQA los conocimientos y

Actividad	Paquete de Trabajo	Entregable	Descripción
		firma EEQA.	habilidades necesarias para la ejecución de sus funciones y asumir sus responsabilidades.
	1.6.3 Seguimiento y Control	1.6.3.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan original del proyecto.
1.7 Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad.	1.7.1 Seguridad de las Aplicaciones.	1.7.1.1 Plan para la revisión de aplicaciones, desde la perspectiva de seguridad.	Establecimiento de las distintas actividades a desarrollar por el equipo de profesionales de la Firma EEQA, para asegurar la correcta gestión de los riesgos vinculados a las aplicaciones y su acceso, principalmente desde Internet.
	1.7.2 Seguridad de la Información.	1.7.2.1 Plan para la revisión de la seguridad de la información.	Definición de las distintas actividades a desarrollar por el equipo de profesionales de la Firma EEQA, para asegurar la integridad, confidencialidad y disponibilidad de la información de sus

Actividad	Paquete de Trabajo	Entregable	Descripción
			clientes.
	1.7.3 Seguridad de la Infraestructura.	1.7.3.1 Plan para la revisión de infraestructura de TI, desde la perspectiva de seguridad.	Establecimiento de las distintas actividades a ejecutar por el equipo de profesionales de la Firma EEQA, para verificar la seguridad y alta disponibilidad de la Infraestructura Tecnológica de sus clientes, considerando para ello las barreras físicas y los mecanismos lógicos de control.
	1.7.4 Seguridad de la Gestión del Recurso Humano.	1.7.4.1 Plan para el seguimiento de la función del recurso humano de TI, desde la perspectiva de seguridad.	Validar la existencia de planes para disminuir la dependencia sobre personal de TI, planes de sucesión del personal, traspaso del conocimiento y segregación de funciones, entre otros aspectos.
	1.7.5 Seguimiento y Control	1.7.5.1 Informe de Control y Seguimiento del Proyecto	Identificar y aplicar las medidas preventivas y correctivas para atender las desviaciones del plan

Actividad	Paquete de Trabajo	Entregable	Descripción
			original del proyecto.
1.8 Entrega del Proyecto.	1.8.1 Firma de aceptación del entregable.	1.8.1.1 Acta de entrega del proyecto.	Formalización de los entregables del proyecto y visto bueno de parte de la Firma EEQA.
	1.8.2 Facturación del Proyecto.	1.8.2.1 Pago de la asesoría técnica del proyecto.	Implica la facturación final del proyecto, debido principalmente a la contratación de una asesoría en el tema de Seguridad Informática.
	1.8.3 Documentación del Proyecto.	1.8.3.1 Documentación de las Lecciones Aprendidas.	Incluye la información sobre las desviaciones presentadas en el proyecto y las acciones correctivas aplicadas.
	1.8.4 Cierre de Adquisiciones.	1.8.4.1 Plan de gestión de las adquisiciones.	Se documentan los acuerdos relacionados con las adquisiciones del proyecto.

Fuente: (El Autor, 2018)

De esta forma, se identifican y se documentan las acciones específicas que se requieren para producir los entregables del proyecto.

Cabe destacar que durante el proceso de estimación de las fechas de las actividades, así como para la definición de los recursos requeridos para su ejecución, se contará con la participación de un asesor tecnológico experto en

seguridad informática, cuyo aporte permitirá desarrollar algunos de los principales entregables del proyecto, entre ellos la creación del “Plan de revisión de los recursos de TI”, específicamente desde la óptica de seguridad.

De esta forma, se procede con la evaluación de la integridad de la información, de la infraestructura tecnológica, de las aplicaciones y de la gestión del recurso humano, todos ellos denominados recursos de TI. Al respecto, se estableció el siguiente cuadro con la planificación efectuada en conjunto con el equipo de trabajo de la Firma EEQA:

Cuadro No. 22: Calendarización de las Actividades del Proyecto

Nombre de la Tarea	Duración	Comienzo	Fin
1. Plan Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI).	74 días	19/02/2018	06/06/2018
1.1 Identificación de Requisitos del Proyecto.	3 días	19/02/2018	21/02/2018
1.1.1 Reunión con la Firma de Consultoría EEQA.	3 días	19/02/2018	21/02/2018
1.1.1.1 Levantamiento de Requisitos Generales del Proyecto.	2 días	19/02/2018	20/02/2018
1.1.1.2 Levantamiento de Requisitos Técnicos del Proyecto.	2 días	20/02/2018	21/02/2018
1.2 Especificación del Marco Normativo.	3 días	22/02/2018	26/02/2018
1.2.1 Legislación Costarricense.	2 días	22/02/2018	23/02/2018
1.2.1.1 Normas Técnicas para la Gestión y el Control de las Tecnologías de Información,	2 días	22/02/2018	23/02/2018

Nombre de la Tarea	Duración	Comienzo	Fin
emitidas por la CGR.			
1.2.1.2 Acuerdo SUGEF 14-17.	2 días	22/02/2018	23/02/2018
1.2.2 Estándares y Marcos de Referencia Internacionales.	3 días	22/02/2018	26/02/2018
1.2.2.1 COBIT - ISACA.	2 días	22/02/2018	23/02/2018
1.2.2.2 ITIL.	2 días	22/02/2018	23/02/2018
1.2.2.3 ISO-27001.	2 días	22/02/2018	23/02/2018
1.2.2.4 Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo Aplicable.	1 día	26/02/2018	26/02/2018
1.3 Implementación de Herramientas Tecnológicas.	14 días	27/02/2018	16/03/2018
1.3.1 Herramientas para el Análisis de Datos.	5 días	27/02/2018	05/03/2018
1.3.1.1 Análisis de viabilidad para la instalación de la herramienta “ACL”.	5 días	27/02/2018	05/03/2018
1.3.1.2 Análisis de viabilidad para la instalación de la herramienta “IDEA”.	5 días	27/02/2018	05/03/2018
1.3.1.3 Análisis de viabilidad para la instalación de la herramienta “TOAD”.	5 días	27/02/2018	05/03/2018
1.3.1.4 Primera Reunión de Seguimiento al Avance del Proyecto.	1 día	05/03/2018	05/03/2018
1.3.2 Herramientas para el Escaneo de Vulnerabilidades.	10 días	05/03/2018	16/03/2018
1.3.2.1 Estudio de herramientas para escaneo de vulnerabilidades en Servidores.	5 días	05/03/2018	09/03/2018
1.3.2.2 Estudio de herramientas	5 días	05/03/2018	09/03/2018

Nombre de la Tarea	Duración	Comienzo	Fin
para escaneo de vulnerabilidades en Redes.			
1.3.2.3 Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos.	5 días	05/03/2018	09/03/2018
1.3.2.4 Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Implementar.	1 día	12/03/2018	12/03/2018
1.3.2.5 Reserva para Contingencia.	4 días	13/03/2018	16/03/2018
1.4 Elaboración y formalización de procedimientos de Auditoría.	17 días	19/03/2018	13/04/2018
1.4.1 Segunda Reunión de Seguimiento al Avance del Proyecto.	1 día	19/03/2018	19/03/2018
1.4.2 Elaboración de Políticas.	5 días	19/03/2018	23/03/2018
1.4.3 Elaboración de Procedimientos.	8 días	26/03/2018	06/04/2018
1.4.4 Tercera Reunión de Seguimiento al Avance del Proyecto.	1 día	26/03/2018	26/03/2018
1.4.5 Cuarta Reunión de Seguimiento al Avance del Proyecto.	1 día	02/04/2018	02/04/2018
1.4.6 Elaboración de Instructivos y Manuales.	3 días	09/04/2018	12/04/2018
1.4.7 Punto de Control No.3: Evaluación de los Requerimientos de Auditoría.	1 día	13/04/2018	13/04/2018
1.5 Definición de Herramienta para la Valoración de Riesgos de TI.	5 días	09/04/2018	13/04/2018
1.5.1 Quinta Reunión de Seguimiento al Avance del Proyecto.	1 día	16/04/2018	16/04/2018
1.5.2 Matriz SEVRI de la Contraloría	2 días	16/04/2018	17/04/2018

Nombre de la Tarea	Duración	Comienzo	Fin
General de la República.			
1.5.3 RISK IT de ISACA.	1 día	18/04/2018	18/04/2018
1.5.4 MARGERIT.	1 día	19/04/2018	19/04/2018
1.5.5 AS/NZS.	1 día	20/04/2018	20/04/2018
1.6 Gestión del Recurso Humano.	2 días	23/04/2018	24/04/2018
1.6.1 Sexta Reunión de Seguimiento al Avance del Proyecto.	1 día	23/04/2018	23/04/2018
1.6.2 Definición del Perfil del Personal de Auditoría de TI.	1 día	23/04/2018	23/04/2018
1.6.3 Capacitación del Personal.	1 día	24/04/2018	24/04/2018
1.7 Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad.	26 días	25/04/2018	31/05/2018
1.7.1 Seguridad de las Aplicaciones.	5 días	25/04/2018	02/05/2018
1.7.2 Séptima Reunión de Seguimiento al Avance del Proyecto.	1 día	30/04/2018	30/04/2018
1.7.3 Seguridad de la Información.	4 días	03/05/2018	08/05/2018
1.7.4 Octava Reunión de Seguimiento al Avance del Proyecto.	1 día	07/05/2018	07/05/2018
1.7.5 Seguridad de la Infraestructura.	5 días	09/05/2018	15/05/2018
1.7.6 Novena Reunión de Seguimiento al Avance del Proyecto.	1 día	14/05/2018	14/05/2018
1.7.7 Seguridad de la Gestión del Recurso Humano.	5 días	17/05/2018	23/05/2018
1.7.8 Décima Reunión de Seguimiento al Avance del Proyecto.	1 día	21/05/2018	21/05/2018
1.7.9 Reserva para Contingencia.	5 días	24/05/2018	30/05/2018
1.7.10 Punto de Control No.4: Evaluación del Plan para la Revisión	1 día	31/05/2018	31/05/2018

Nombre de la Tarea	Duración	Comienzo	Fin
del SGSI.			
1.8 Entrega del Proyecto	3 días	04/06/2018	06/06/2018
1.8.1 Firma de Aceptación de los Entregables del Proyecto.	1 día	04/06/2018	04/06/2018
1.8.2 Facturación del Proyecto.	1 día	04/06/2018	04/06/2018
1.8.3 Documentos del Proyecto.	1 día	05/06/2018	05/06/2018
1.8.3.1 Documentación de las Lecciones Aprendidas.	1 día	05/06/2018	06/06/2018
1.8.4 Cierre de Adquisiciones.	1 día	06/06/2018	06/06/2018

Fuente: (El Autor, 2018)

Por otra parte, se estableció una secuencia lógica de las actividades que forman parte del plan, determinándose tanto las actividades sucesoras como las predecesoras, lo cual se muestra a continuación:

Cuadro No. 23: Secuencia de las Actividades del Proyecto

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
1	1.1.1.1	Levantamiento de Requisitos Generales del Proyecto	-	3,4,5,6 y 7	Director del Proyecto, Socios de la Firma, Gerente de Auditoría, Equipo de Auditores de la

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
					Firma, Asesor experto en Seguridad Informática.
2	1.1.1.2	Levantamiento de Requisitos Técnicos del Proyecto	-	3,4,5,6 y 7	Director del Proyecto, Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
3	1.2.1.1	Revisión de las Normas Técnicas para la Gestión y el Control de las TI, emitidas por la CGR	1,2	8,9,10,11,12 y 13	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
4	1.2.1.2	Revisión del Acuerdo SUGEF 14-17	1,2	8,9,10,11,12 y 13	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
5	1.2.2.1	Informe COBIT - ISACA	1,2	8,9,10,11,12 y 13	Gerente de Auditoría, Equipo de Auditores de la

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
					Firma EEQA.
6	1.2.2.2	Informe ITIL	1,2	8,9,10,11,12 y 13	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
7	1.2.2.3	Informe ISO-27001	1,2	8,9,10,11,12 y 13	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
8	1.3.1.1	Análisis de viabilidad para la instalación de la herramienta “ACL”	3,4,5,6 y 7	14,15 y 16	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
9	1.3.1.2	Análisis de viabilidad para la instalación de la herramienta “IDEA”	3,4,5,6 y 7	14,15 y 16	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
10	1.3.1.3	Análisis de viabilidad para la instalación de la herramienta “TOAD”	3,4,5,6 y 7	14,15 y 16	Gerente de Auditoría, Equipo de Auditores de la Firma EEQA.
11	1.3.2.1	Informe sobre escaneo de Vulnerabilidades	3,4,5,6 y 7	14,15 y 16	Asesor experto en Seguridad Informática.

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
		de Servidores (Microsoft, UNIX, LINUX)			
12	1.3.2.2	Informe sobre escaneo de Vulnerabilidades de Redes (CISCO, JUNIPER, HUAWEI)	3,4,5,6 y 7	14,15 y 16	Asesor experto en Seguridad Informática.
13	1.3.2.3	Informe sobre escaneo de vulnerabilidades de Bases de Datos (Oracle, SQL Server, MySQL)	3,4,5,6 y 7	14,15 y 16	Asesor experto en Seguridad Informática
14	1.4.1	Elaboración de Políticas.	8,9,10,11,12 y 13	17,18,19 y 20	Socios de la Firma, Gerente de Auditoría.
15	1.4.2	Elaboración de Procedimientos.	8,9,10,11,12 y 13	17,18,19 y 20	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
16	1.4.3	Elaboración de	8,9,10,11,12	17,18,19 y	Gerente de

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
		Instructivos y Manuales.	y 13	20	Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
17	1.5.1	Revisión de la Matriz SEVRI de la Contraloría General de la República.	14,15 y 16	21 y 22	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
18	1.5.2	Revisión de la metodología “RISK IT” de ISACA.	14,15 y 16	21 y 22	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
19	1.5.3	Revisión del marco de referencia “MARGERIT	14,15 y 16	21 y 22	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
					Seguridad Informática.
20	1.5.4	Revisión de la Norma “AS/NZS”.	14,15 y 16	21 y 22	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
21	1.6.1	Definición del Perfil del personal de Auditoría de TI.	17,18,19 y 20	23,24,25 y 26	Director del Proyecto, Socios de la Firma, Gerente de Auditoría, Encargada del Gestión de Talento Humano de EEQA.
22	1.6.2	Capacitación del Personal.	17,18,19 y 20	23,24,25 y 26	Director del Proyecto, Socios de la Firma, Gerente de Auditoría, Encargada del Gestión de Talento Humano de

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
					EEQA.
23	1.7.1	Plan para la revisión de aplicaciones, desde la perspectiva de seguridad.	21 y 22	27,28,29 y 30	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
24	1.7.2	Plan para la revisión de la seguridad de la información.	21 y 22	27,28,29 y 30	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
25	1.7.3	Plan para la revisión de infraestructura de TI, desde la perspectiva de seguridad.	21 y 22	27,28,29 y 30	Gerente de Auditoría, Equipo de Auditores de la Firma, Asesor experto en Seguridad Informática.
26	1.7.4	Plan para el seguimiento de la función del recurso humano	21 y 22	27,28,29 y 30	Gerente de Auditoría, Equipo de Auditores de la

ID	Código EDT	Actividad	Predecesora	Sucesora	Recursos
		de TI, desde la perspectiva de seguridad.			Firma, Asesor experto en Seguridad Informática.
27	1.8.1	1.8.1 Firma de aceptación del entregable.	23,24,25 y 26	-	Director del Proyecto, Socios de la Firma, Gerente de Auditoría.
28	1.8.2	1.8.2 Facturación del Proyecto.	23,24,25 y 26	-	Director del Proyecto, Socios de la Firma, Gerente de Auditoría.
29	1.8.3.1	Documentación de las Lecciones Aprendidas.	23,24,25 y 26	-	Director del Proyecto, Socios de la Firma, Gerente de Auditoría.
30	1.8.4	Cierre de Adquisiciones.	23,24,25 y 26	-	Director del Proyecto, Socios de la Firma, Gerente de Auditoría.

Fuente: (El Autor, 2018)

Finalmente, se desarrolla el cronograma del proyecto “Plan de Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información” para la firma de consultoría EEQA, el cual se constituye como uno de los principales entregables del proceso de gestión del tiempo del proyecto:

Cuadro No. 24: Cronograma del Proyecto

	Nombre	Duración	Inicio	Terminado	Predecesores
1	**Plan de Dirección para Auditar un Sistema de Gestión de Seguridad de**	74 days?	**19/02/18 8:00**	**6/06/18 17:00**	
2	**Identificación de Requisitos del Proyecto**	3 days?	**19/02/18 8:00**	**21/02/18 17:00**	
3	**Reunión con la Firma de Consultoría EEQA**	3 days?	**19/02/18 8:00**	**21/02/18 17:00**	
4	Levantamiento de Requisitos Generales del Proyecto	2 days?	19/02/18 8:00	20/02/18 17:00	
5	Levantamiento de Requisitos Técnicos del Proyecto	2 days?	20/02/18 8:00	21/02/18 17:00	
6	**Especificación del Marco Normativo**	3 days?	**22/02/18 8:00**	**26/02/18 17:00**	
7	**Legislación Costarricense**	2 days?	**22/02/18 8:00**	**23/02/18 17:00**	
8	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información	2 days?	22/02/18 8:00	23/02/18 17:00	4;5
9	Acuerdo SUGEF 14-17	2 days?	22/02/18 8:00	23/02/18 17:00	4;5
10	**Estándares y Marcos de Referencia Internacionales**	3 days?	**22/02/18 8:00**	**26/02/18 17:00**	
11	COBIT - ISACA	2 days?	22/02/18 8:00	23/02/18 17:00	4;5
12	ITIL	2 days?	22/02/18 8:00	23/02/18 17:00	4;5
13	ISO-27001	2 days?	22/02/18 8:00	23/02/18 17:00	4;5
14	Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo A	1 day	26/02/18 8:00	26/02/18 17:00	
15	HITO I - REQUERIMIENTOS DE LA METODOLOGÍA	0 days	26/02/18 8:00	26/02/18 8:00	
16	**Implementación de Herramientas Tecnológicas**	14 days?	**27/02/18 8:00**	**16/03/18 17:00**	
17	**Herramientas para el Análisis de Datos**	5 days?	**27/02/18 8:00**	**5/03/18 17:00**	
18	Análisis de viabilidad para la instalación de la herramienta "ACL"	5 days?	27/02/18 8:00	5/03/18 17:00	8;9;11;12;13
19	Análisis de viabilidad para la instalación de la herramienta "IDEA"	5 days?	27/02/18 8:00	5/03/18 17:00	8;9;11;12;13
20	Análisis de viabilidad para la instalación de la herramienta "TOAD"	5 days?	27/02/18 8:00	5/03/18 17:00	8;9;11;12;13
21	Primera Reunión de Seguimiento al Avance del Proyecto	1 day?	5/03/18 8:00	5/03/18 17:00	
22	**Herramientas para el Escaneo de Vulnerabilidades**	10 days?	**5/03/18 8:00**	**16/03/18 17:00**	
23	Estudio de herramientas para escaneo de vulnerabilidades en Servidores	5 days?	5/03/18 8:00	9/03/18 17:00	8;9;11;12;13
24	Estudio de herramientas para escaneo de vulnerabilidades en Redes	5 days?	5/03/18 8:00	9/03/18 17:00	8;9;11;12;13
25	Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos	5 days?	5/03/18 8:00	9/03/18 17:00	8;9;11;12;13
26	Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Impleme	1 day?	12/03/18 8:00	12/03/18 17:00	
27	HITO II - IMPLEMENTACIÓN DE HERRAMIENTAS	0 days	12/03/18 8:00	12/03/18 8:00	
28	Reserva para Contingencia	4 days	13/03/18 8:00	16/03/18 17:00	
29	**Elaboración y Formalización de Procedimientos de Auditoría**	17 days?	**19/03/18 8:00**	**13/04/18 17:00**	
30	Segunda Reunión de Seguimiento al Avance del Proyecto	1 day?	19/03/18 8:00	19/03/18 17:00	
31	Elaboración de Políticas	5 days?	19/03/18 8:00	23/03/18 17:00	7;10;16;22
32	Elaboración de Procedimientos	8 days?	26/03/18 8:00	6/04/18 17:00	7;10;16;22
33	Tercera Reunión de Seguimiento al Avance del Proyecto	1 day?	26/03/18 8:00	26/03/18 17:00	
34	Cuarta Reunión de Seguimiento al Avance del Proyecto	1 day?	2/04/18 8:00	2/04/18 17:00	
35	Elaboración de Instructivos y Manuales	3 days?	9/04/18 8:00	12/04/18 17:00	7;10;16;22
36	Punto de Control No.3: Evaluación de los Procedimientos de Auditoría	1 day?	13/04/18 8:00	13/04/18 17:00	
37	HITO III - CREACIÓN DE PROCEDIMIENTOS DE AUDITORÍA	0 days	13/04/18 8:00	13/04/18 8:00	
38	**Definición de Herramienta para la Valoración de Riesgos de TI**	5 days?	**16/04/18 8:00**	**20/04/18 17:00**	
39	Quinta Reunión de Seguimiento al Avance del Proyecto	1 day?	16/04/18 8:00	16/04/18 17:00	
40	Matriz SEVRI de la Contraloría General de la República	2 days?	16/04/18 8:00	17/04/18 17:00	7;10;16;22
41	RISK IT de ISACA	1 day?	18/04/18 8:00	18/04/18 17:00	7;10;16;22
42	MARGERIT	1 day?	19/04/18 8:00	19/04/18 17:00	7;10;16;22
43	AS/NZS	1 day?	20/04/18 8:00	20/04/18 17:00	7;10;16;22
44	**Gestión del Recurso Humano**	2 days?	**23/04/18 8:00**	**24/04/18 17:00**	
45	Sexta Reunión de Seguimiento al Avance del Proyecto	1 day?	23/04/18 8:00	23/04/18 17:00	
46	Definición del Perfil del Personal de Auditoría de TI	1 day?	23/04/18 8:00	23/04/18 17:00	16;22;29;38
47	Capacitación del Personal	1 day?	24/04/18 8:00	24/04/18 17:00	
48	**Creación del Plan de Revisión de los Recursos de TI, desde la perspe**	26 days?	**25/04/18 8:00**	**31/05/18 17:00**	
49	Seguridad de las Aplicaciones	5 days?	25/04/18 8:00	2/05/18 17:00	16;22;29;38
50	Séptima Reunión de Seguimiento al Avance del Proyecto	1 day?	30/04/18 8:00	30/04/18 17:00	
51	Seguridad de la Información	4 days?	3/05/18 8:00	8/05/18 17:00	16;22;29;38
52	Octava Reunión de Seguimiento al Avance del Proyecto	1 day?	7/05/18 8:00	7/05/18 17:00	
53	Seguridad de la Infraestructura	5 days?	9/05/18 8:00	15/05/18 17:00	16;22;29;38
54	Novena Reunión de Seguimiento al Avance del Proyecto	1 day?	14/05/18 8:00	14/05/18 17:00	
55	Seguridad de la Gestión del Recurso Humano	5 days?	17/05/18 8:00	23/05/18 17:00	16;22;29;38
56	Décima Reunión de Seguimiento al Avance del Proyecto	1 day?	21/05/18 8:00	21/05/18 17:00	
57	Reserva para Contingencia	5 days	24/05/18 8:00	30/05/18 17:00	
58	Punto de Control No.4: Evaluación del Plan para la Revisión del SGSI	1 day?	31/05/18 8:00	31/05/18 17:00	
59	HITO IV - FORMULACIÓN DEL PLAN DE REVISIÓN DEL SGSI	0 days	31/05/18 8:00	31/05/18 8:00	
60	**Entrega del Proyecto**	3 days?	**4/06/18 8:00**	**6/06/18 17:00**	
61	Firma de Aceptación de los Entregables del Proyecto	1 day?	4/06/18 8:00	4/06/18 17:00	29;48
62	Facturación del Proyecto	1 day?	4/06/18 8:00	4/06/18 17:00	29;48
63	**Documentos del Proyecto**	1 day?	**5/06/18 8:00**	**5/06/18 17:00**	
64	Documentación de las Lecciones Aprendidas	1 day?	5/06/18 8:00	5/06/18 17:00	29;48
65	Cierre de Adquisiciones	1 day?	6/06/18 8:00	6/06/18 17:00	29;48

Fuente: (El Autor, 2018)

Al analizar el cronograma del proyecto se debe hacer referencia a las siguientes condiciones que se valoraron para su formulación:

- No se consideraron como días laborales los sábados y domingos.

- De acuerdo con los artículos 147, 148, 149, 150, 152 del Código de Trabajo en Costa Rica, donde se establecen los días hábiles para el trabajo, así como los días feriados, no se calendarizó ninguna actividad en los días:

  29 y 30 de marzo por corresponder al jueves y viernes de la semana santa.
  11 de abril, día de Juan Santamaría.
  01 de mayo, día del Trabajo.

- La jornada laboral se extiende de 8:00 a.m. a 5:00 p.m.

Adicionalmente, se aplicó un filtro en la herramienta “OpenProj” utilizada para la formulación del cronograma de actividades del proyecto, para identificar las actividades que forman parte de la “Ruta Crítica”, acentuada a través del color rojo:

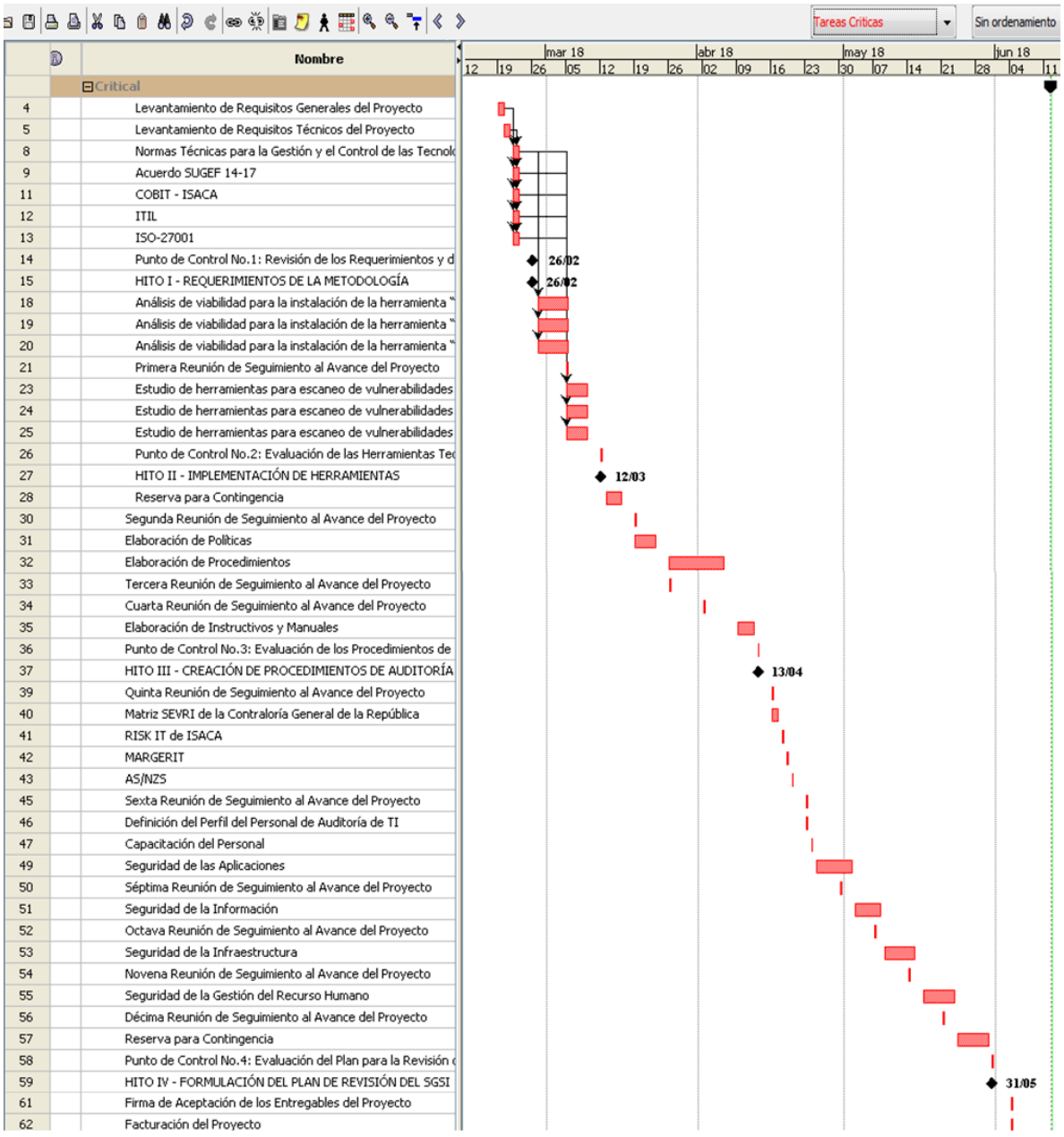


Figura No.7. Ruta Crítica del Proyecto

Fuente: (El Autor, 2018)

Su importancia radica en que la duración de la “Ruta Crítica” determina la duración del proyecto entero. Cualquier retraso en un elemento de la ruta crítica afecta a la fecha de conclusión planificada.

En caso que el Director del Proyecto considere necesario reducir los tiempos de ejecución del proyecto, se podría aplicar la técnica de compresión del cronograma, mediante la incorporación de recursos adicionales que posibiliten recortar la duración de tareas especificas; por ejemplo, a través del pago de de horas extras; asimismo, también existe la posibilidad de compresión del cronograma por medio de la ejecución de trabajos de forma paralela.

El análisis PERT fue el instrumento utilizado para determinar la duración esperada de cada actividad, donde una vez más se acudió al juicio experto de quienes forman parte del proyecto, tomándose en consideración la complejidad técnica de las actividades, los recursos necesarios y sus calendarios de utilización.

Cuadro No. 25: Duración Esperada de las Actividades del Proyecto

EDT	Actividad	Duración Optimista	Duración Más Probable	Duración Pesimista	Duración Esperada
1.1.1.1	Levantamiento de Requisitos Generales del Proyecto	2	2	4	2
1.1.1.2	Levantamiento de Requisitos Técnicos del Proyecto	2	2	4	2
1.2.1.1	Revisión de las Normas Técnicas para la Gestión y el Control de las TI, emitidas por la CGR	2	2	4	2
1.2.1.2	Revisión del	2	2	4	2

	Acuerdo SUGEF 14-17				
1.2.2.1	Informe COBIT – ISACA	2	2	4	2
1.2.2.2	Informe ITIL	2	2	4	2
1.2.2.3	Informe ISO-27001	2	2	4	2
1.3.1.1	Análisis de viabilidad para la instalación de la herramienta “ACL”	5	5	10	6
1.3.1.2	Análisis de viabilidad para la instalación de la herramienta “IDEA”	5	5	10	6
1.3.1.3	Análisis de viabilidad para la instalación de la herramienta “TOAD	5	5	10	6
1.3.2.1	Informe sobre escaneo de Vulnerabilidades de Servidores (Microsoft, UNIX, LINUX)	5	5	10	6
1.3.2.2	Informe sobre escaneo de Vulnerabilidades de Redes (CISCO, JUNIPER, HUAWEI)	5	5	10	6
1.3.2.3	Informe sobre	5	5	10	6

	escaneo de vulnerabilidades de Bases de Datos (Oracle, SQL Server, MySQL)				
1.4.1	Elaboración de Políticas de Auditoría.	5	5	10	6
1.4.2	Elaboración de Procedimientos.	8	8	16	9
1.4.3	Elaboración de Instructivos y Manuales.	3	3	6	4
1.5.1	Revisión de la Matriz SEVRI de la Contraloría General de la República.	2	2	4	2
1.5.2	Revisión de la metodología “RISK IT” de ISACA	1	1	2	1
1.5.3	Revisión del marco de referencia “MARGERIT	1	1	2	1
1.5.4	Revisión de la Norma “AS/NZS”.	1	1	2	1
1.6.1	Definición del Perfil del personal de Auditoría de TI.	1	1	2	1
1.6.2	Capacitación del Personal.	1	1	2	1
1.7.1	Plan para la revisión	5	5	10	6

	de aplicaciones, desde la perspectiva de seguridad				
1.7.2	Plan para la revisión de la seguridad de la información.	4	4	8	5
1.7.3	Plan para la revisión de infraestructura de TI, desde la perspectiva de seguridad.	5	5	10	6
1.7.4	Plan para el seguimiento de la función del recurso humano de TI, desde la perspectiva de seguridad.	5	5	10	6
1.8.1	Firma de aceptación del entregable.	1	1	2	1
1.8.2	Facturación del Proyecto.	1	1	2	1
1.8.3.1	Documentación de las Lecciones Aprendidas.	1	1	2	1
1.8.4	Cierre de Adquisiciones.	1	1	2	1

Fuente: (El Autor, 2018)

El seguimiento y control de la duración de las actividades es una función fundamental bajo la responsabilidad del Director del Proyecto, en procura de efectuar el consumo eficaz y eficiente de los recursos a disposición del equipo de trabajo. Por ende, el seguimiento respectivo debe efectuarse diariamente, con la finalidad de atender oportunamente las desviaciones del plan.

4.4 Plan de Gestión del Costo

La Gestión de los Costos del Proyecto *"se ocupa principalmente del costo de los recursos necesarios para completar las actividades del proyecto."* (PMI, 2013, pág. 195). Planificar la gestión de los costos debe efectuarse durante las etapas iniciales de la planificación de un proyecto y para tales efectos, se creó el siguiente plan de la gestión de los costos del proyecto, cuyo principal resultado es el presupuesto con el que se contará para concluir las actividades que se indican en el cronograma y que será proporcionado por los socios de la Firma EEQA a través de financiamiento propio.

La estimación de costos de las actividades involucra una evaluación cuantitativa de los costos probables que se requieren para completar el trabajo del proyecto, considerando para ello tanto los costos directos como indirectos; asimismo, se utilizará como insumo la EDT desarrollada en el punto 4.1 del presente documento, de forma tal que las estimaciones de costos se sumen de conformidad con los paquetes de trabajo previamente definidos.

Previo a la presentación de los costos del proyecto, se establecerán los estándares a partir de los cuales se va a definir el presupuesto:

• El Dólar Estadounidense ($) corresponde a la unidad monetaria a utilizar para la formulación del presupuesto.
• Se utilizan horas para medir el trabajo del recurso humano.

• El grado de exactitud de los estimados será de cero decimales (números enteros).

Adicionalmente, el costo unitario de cada recurso y material a utilizar durante el proyecto, se consigna en el siguiente cuadro:

Cuadro No. 26: Costo Unitario del Recurso Humano

Recurso	Costo/Hora
Director del Proyecto	$25
Personal de Auditoría de la Firma EEQA	$15
Personal Administrativo de la Firma EEQA	$15
Encargada de la Gestión de Talento Humano	$15
Asesor Tecnológico	$30

Fuente: (El Autor, 2018)

Cuadro No. 27: Costo Unitario de los Recursos, Materiales y Herramientas

Recurso/Herramienta	Costo
Curso de Fundamentos ITIL para la gestión de servicios de TI.	$ 750
Libro Manual de Revisión CISM, formulado por ISACA.	$ 140
Servicios de Telecomunicaciones (Internet).	$ 100
Telefonía Celular	$ 100
Kilometraje	$ 200

Fuente: (El Autor, 2018)

En relación con los rubros antes citados, se aclara que lo concerniente al suministro del Internet (Servicios de Telecomunicaciones), el reconocimiento del pago de la telefonía celular y el pago del kilometraje, únicamente se otorgarán al Director del Proyecto y al Asesor en el tema de seguridad informática, por cuanto son los únicos miembros del equipo del proyecto que corresponde a personal externo de la Firma EEQA.

El resto de personas participantes son funcionarios de la empresa, por lo que para efectos del presupuesto del proyecto, sólo se consideran las horas de trabajo invertidas en el desarrollo del plan de auditoría. Cabe indicar que ningún funcionario de la Firma EEQA trabajará exclusivamente en el proyecto; por el contrario, su horario de trabajo se fracciona entre la prestación de servicios profesionales a clientes y la implementación del proyecto. Por otra parte, el hardware, software y demás utilitarios requeridos, fueron adquiridos con anterioridad y forman parte de los activos de la empresa, en ningún momento su compra se originó por el desarrollo del proyecto.

Cuadro No. 28: Desglose del Presupuesto del Proyecto

Código EDT	Descripción de la Actividad	Duración	Valor
1	**Plan de Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI)**	**74 días**	**$ 26.778**
1.1	**Identificación de Requisitos del Proyecto**	**3 días**	**$ 3.225**
1.1.1	Reunión con la Firma de	3 días	$ 1381

	Consultoría EEQA		
1.1.1.1	Levantamiento de Requisitos Generales del Proyecto	2 días	$ 922
1.1.1.2	Levantamiento de Requisitos Técnicos del Proyecto	2 días	$ 922
1.2	**Especificación del Marco Normativo**	**3 días**	**$ 1.938**
1.2.1	Legislación Costarricense	2 días	$ 188
1.2.1.1	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR	2 días	$ 188
1.2.1.2	Acuerdo SUGEF 14-17	2 días	$ 188
1.2.2	Estándares y Marcos de Referencia Internacionales	3 días	$ 188
1.2.2.1	COBIT - ISACA	2 días	$ 188
1.2.2.2	ITIL	2 días	$ 188
1.2.2.3	ISO-27001	2 días	$ 188
1.2.2.4	Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo Aplicable.	1 día	$ 622
1.3	**Implementación de Herramientas Tecnológicas**	**14 días**	**$ 5.406**
1.3.1	Herramientas para el Análisis de Datos	5 días	$ 598
1.3.1.1	Análisis de viabilidad para la instalación de la herramienta “ACL”	5 días	$ 598
1.3.1.2	Análisis de viabilidad para la instalación de la herramienta	5 días	$ 598

	“IDEA”		
1.3.1.3	Análisis de viabilidad para la instalación de la herramienta “TOAD”	5 días	$ 598
1.3.2	Herramientas para el Escaneo de Vulnerabilidades	5 días	$ 598
1.3.2.1	Estudio de herramientas para escaneo de vulnerabilidades en Servidores	5 días	$ 598
1.3.2.2	Estudio de herramientas para escaneo de vulnerabilidades en Redes	5 días	$ 598
1.3.2.3	Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos	5 días	$ 598
1.3.2.4	Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Implementar.	1 día	$ 622
1.4	**Elaboración y formalización de procedimientos de Auditoría**	**17 días**	**$ 5.662**
1.4.1	Elaboración de Políticas	5 días	$ 1.200
1.4.2	Elaboración de Procedimientos	8 días	$ 3.120
1.4.3	Elaboración de Instructivos y Manuales	3 días	$ 720
1.4.7	Punto de Control No.3: Evaluación de los Requerimientos de Auditoría.	1 día	$ 622

1.5	**Definición de Herramienta para la Valoración de Riesgos de TI**	**5 días**	**$ 2.232**
1.5.1	Matriz SEVRI de la Contraloría General de la República	2 día	$ 446
1.5.2	RISK IT de ISACA	1 día	$ 894
1.5.3	MARGERIT	1 día	$ 446
1.5.4	AS/NZS	1 día	$ 446
1.6	**Gestión del Recurso Humano**	**2 días**	**$ 1.244**
1.6.1	Definición del Perfil del Personal de Auditoría de TI	1 día	$ 622
1.6.2	Capacitación del Personal	1 día	$ 622
1.7	**Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad**	**26 días**	**$ 6.646**
1.7.1	Seguridad de las Aplicaciones	5 días	$ 1,506
1.7.2	Seguridad de la Información	4 días	$ 1.506
1.7.3	Seguridad de la Infraestructura	5 días	$ 1.506
1.7.4	Seguridad de la Gestión del Recurso Humano	5 días	$ 1.506
1.7.10	Punto de Control No.4: Evaluación del Plan para la Revisión del SGSI.	1 día	$ 622
1.8	**Entrega del Proyecto**	**3 días**	**$ 425**
1.8.1	Firma de Aceptación de los Entregables del Proyecto	1 día	$ 85
1.8.2	Facturación del Proyecto	1 día	$ 85

1.8.3	Documentos del Proyecto	1 día	$ 85
1.8.3.1	Documentación de las Lecciones Aprendidas	1 día	$ 85
1.8.4	Cierre de Adquisiciones	1 día	$ 85

Fuente: (El Autor, 2018)

De conformidad con el cuadro supracitado, se procede a graficar las 4 etapas del proyecto, para la visualización de los puntos de mayor relevancia desde la perspectiva de inversión según la fase del proyecto:

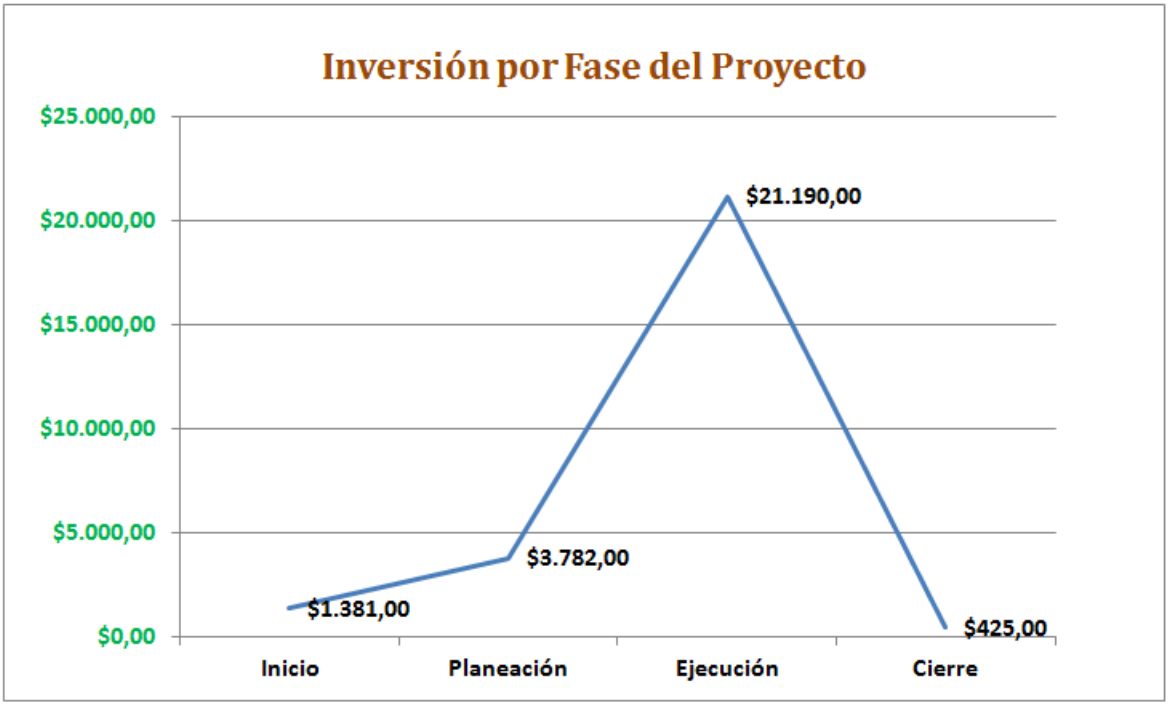


Figura No.8. Inversión por Fase del Proyecto

Fuente: (El Autor, 2018)

Finalmente, el cuadro adjunto resume los costos del proyecto y el presupuesto requerido para completar satisfactoriamente cada una de las actividades consignadas en el cronograma del proyecto; asimismo, se indican las reservas de contingencia y de gestión del proyecto:

Cuadro No. 29: Presupuesto Final del Proyecto

Actividad	Costo
Fase de Inicio	$ 1.381,00
Fase de Planeamiento	$ 3.782,00
Fase de Ejecución	$ 21.190,00
Fase de Cierre	$ 425,00
Subtotal	**$ 26.778,00**
Reserva de Contingencia 5%	$ 1.339
Costo Total del Proyecto	**$ 28.117**
Reserva de Gestión 3%	$ 844
Presupuesto Final del Proyecto	**$ 28.961**

Fuente: (El Autor, 2018)

Acorde con las buenas prácticas de la gestión de proyectos, diariamente se debe controlar el costo de cada una de las actividades como medida para salvaguardar el consumo razonable de los recursos económicos del proyecto. Para ello, se utilizarán el “Valor Planeado” (Línea Base de Costo o Presupuesto), el “Valor Ganado” (El trabajo realizado o avance expresado en costos por actividad” y el “Valor Actual” (El gasto registrado actualmente), para así poder determinar si el proyecto está costando menos o más según lo planificado. Una vez obtenida esta información, se establecerán oportunamente las acciones pertinentes para corregir cualquier desviación que se pudiera presentar, en caso de ser necesario.

4.5 Plan de Gestión de la Calidad

La Gestión de la Calidad del Proyecto incluye los procesos y actividades de la organización ejecutora que establecen las políticas de calidad, los objetivos y las responsabilidades de calidad para que el proyecto satisfaga las necesidades para las que fue acometido. (PMI, 2013). Para ello, se basa en políticas y procedimientos para implementar el sistema de gestión de la calidad en una organización, así como las actividades de mejora continua del proceso, en procura de alcanzar y validar los requisitos del proyecto.

En lo que respecta al plan de auditoría a desarrollar, los socios de la firma han sido claros al afirmar que el mismo únicamente podrá ser implementado si cada uno de los criterios de calidad se cumplen acorde con los indicadores instaurados, máxime cuando la naturaleza de su negocio es brindar asesorías de conformidad a las buenas prácticas y normas aceptadas globalmente.

Es por esta razón que se desarrollaron sesiones de trabajos con el personal de la Firma EEQA, con la finalidad de establecer formalmente los factores críticos de éxito del proyecto, los cuales se muestran a través del siguiente cuadro:

Cuadro No. 30: Factores Relevantes de Calidad del Proyecto

Tipo	Factor	Definición del Factor	Objetivo de Calidad
Proceso	Normas técnicas para la gestión y el control de las Tecnologías de Información. Acuerdo SUGEF	La auditoría a desarrollar, debe ser congruente con el Marco Normativo Costarricense.	Cumplir con los lineamientos establecidos por la Contraloría General de la República y por la SUGEF.

Tipo	Factor	Definición del Factor	Objetivo de Calidad
	14-17		
Proceso	COBIT ITIL ISO-27001	Se debe dar seguimiento a las buenas prácticas consignadas en los marcos de referencia de COBIT, ITIL y en el estándar ISO-27001.	Aplicar los estándares y marcos de referencia sobre las buenas prácticas, en el desarrollo de la auditoría en Tecnologías de Información.
Técnico	Formato de Reportes	Todas las herramientas de análisis de datos y de escaneo de vulnerabilidades que adopte la firma, deben generar reportes en formato “PDF” o “HTML”.	Extracción de los datos de las herramientas tecnológicas a implementar, en un formato legible para el cliente.
Técnico	Herramientas Tecnológicas	Automatización de tareas, ya sea mediante productos licenciados como Open Source.	Implementar al menos una herramientas tecnológica para el análisis de datos y una herramienta para la identificación de

Tipo	Factor	Definición del Factor	Objetivo de Calidad
			vulnerabilidades.
Costo	Presupuesto	El proyecto debe concluir acorde con el presupuesto definido.	Efectuar el cierre del proyecto dentro de los costos establecidos para no impactar el presupuesto asignado al proyecto.
Tiempo	Cronograma	El proyecto debe finalizar según las fechas del cronograma aprobado.	Cerrar el proyecto dentro del tiempo establecido para iniciar el proceso de inscripción en el registro de oferentes de la SUGEF.
Capacitación	Validación de Conocimientos	Los funcionarios de la Firma EEQA, deben aprobar el plan de capacitación proporcionado por la empresa.	Medir el nivel de conocimiento de los funcionarios que serán responsable de ejecutar la auditoría del SGSI.

Fuente: (El Autor, 2018)

Con la finalidad de asegurar la calidad del proyecto, se incorporó el uso de “Hoja de Verificación de Contenido”, la cual corresponde a una herramienta 7QC utilizada en el contexto del Ciclo PDCA, para atender problemas relacionados con la calidad. La misma fue aplicada durante una de las actividades de mayor relevancia dentro del proyecto, la cual corresponde a la creación del “Plan de Revisión de los Recursos de TI”, desde la perspectiva de seguridad.

De esta forma, se aplicó dicha herramienta como lista de comprobación al recolectar datos que permitieron comprobar que tareas fundamentales en la revisión del Sistema de Gestión de Seguridad de la Información, fueran consideradas como parte del plan de auditoría que pretende comercializar la Firma de consultoría EEQA.

Cuadro No. 31: Formulario para la Verificación de Contenido

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	**Criterio de Evaluación**	**Valoración**		**Recomendaciones**
		Presente	**No Presente**	
1	Se evalúa la razonabilidad y el cumplimiento de las Disposiciones Informáticas y sus procedimientos.			
2	Se revisan los lineamientos para prevenir las fugas de			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	información.			
3	Se revisa el software instalado en los equipos de cómputo, a través del uso de una herramienta automatizada. Verificar que se mantenga actualizado el inventario de software y activos de TI.			
4	Se revisan los perfiles y roles de los usuarios a la red y equipo, para el acceso a la información, según las políticas de acceso establecidas.			
5	Se monitorea mediante alguna herramienta automatizada, si se han presentado accesos no autorizados, permisos de usuarios y recursos			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	compartidos.			
6	Se evalúan y monitorean los puertos de comunicación y accesos de los servidores que han sido autorizados por la organización.			
7	Se determina la existencia y validez de certificados “SSL para el sitio Web y correo electrónico, entre otros recursos.			
8	Se verifica la existencia y el cumplimiento de estándares para el Desarrollo de Sistemas, de conformidad con las mejores prácticas y desde una perspectiva de Seguridad de la Información.			
9	Se revisan las restricciones a los cambios en los paquetes de software de			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	control de versiones.			
10	Se revisa el control de acceso al código fuente de los programas.			
11	Se evalúa el funcionamiento de las UPS implementadas y se determina si existen alertas automatizadas para el monitoreo del recurso.			
12	Se efectúa la revisión de la bitácora de acceso al Data Center y de otras áreas restringidas.			
13	Se verifica la fecha de vencimiento de los extintores, así como el funcionamiento de componentes adicionales como son el des-humedecedor, lámparas de emergencia y sistemas de			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	alerta, entre otros dispositivos que normalmente se ubican en un Data Center.			
14	Se evalúa los perfiles de acceso a Internet, así como las bitácoras del recurso.			
15	Se evalúa las políticas de acceso implementadas a través de los equipos Firewall.			
16	Se determina la razonabilidad de los procedimientos para la gestión de claves “Súper-Usuario”, para la administración de Servidores y de Bases de Datos, entre otros.			
17	Se revisa el control de acceso al Sistema Operativo			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	de los equipos, considerando los procedimientos seguros de inicio de sesión, mecanismo de identificación (perfiles) y autenticación de usuario, mecanismo de gestión de contraseñas, mecanismo de desconexión automática de sesión y el mecanismo de limitación del tiempo de conexión, entre otros.			
18	Se analiza el desempeño de Servidores y Sistema Operativo Linux, obteniendo un detalle general de los procesos, E/S, uso de memoria/swap, estado del sistema y actividad del CPU.			
19	Se revisan las condiciones generales de las Bases de			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	**Criterio de Evaluación**	**Valoración**		**Recomendaciones**
		Presente	**No Presente**	
	Datos, independientemente si son Oracle, SQL Server, MySQL, entre otras.			
20	Se analizan los roles y perfiles de Bases de Datos.			
21	Se monitorea la base de datos a través de la ejecución de scripts, por ejemplo, de espacio, de objetos inválidos, roles asignados y del tablespace “SYSTEM”, entre otros.			
22	Se evalúa el funcionamiento y configuración de la Infraestructura Tecnológica de almacenamiento de datos, como es el caso de equipos “SAN” o “NAS”.			
23	Se evalúa el funcionamiento de la Infraestructura Tecnológica de respaldo,			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	considerando la generación de pruebas de integridad y restauración.			
24	Se corrobora la existencia de un Sitio Alterno de TI.			
25	Se verifica que el Sitio Alterno mantenga las condiciones necesarias para la ejecución del Plan de Continuidad de la organización que es objeto de la auditoría.			
26	Se ejecutan análisis de vulnerabilidades utilizando herramientas disponibles, tales como NESSUS o GFI Languard, entre otras.			
27	Se analiza la configuración del Active Directory, considerando la redundancia del recurso y la ejecución de			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	pruebas de restauración de objetos.			
28	Se monitorea la aplicación de actualizaciones de Microsoft Windows, a través de plataformas tales como “WSUS” y “SCCM”.			
29	Se verifica que el Antivirus se encuentre debidamente actualizado, en cada una de las terminales de la organización.			
30	Se realiza el monitoreo de las bitácoras de la consola de antivirus.			
31	Se vigila el desempeño del Servidor de Correo Electrónico y del estado de los buzones de los usuarios.			
32	Se evalúan los procedimientos de acciones			

Hoja de Verificación de Contenido		
Firma Consultora EEQA		
Fecha:	**Nombre del Proyecto:**	**Detalle de la Evaluación:**
	Plan de Dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información	Revisión de las actividades consignadas en el “Plan de Revisión de los Recursos de TI”.

No.	Criterio de Evaluación	Valoración		Recomendaciones
		Presente	No Presente	
	en caso de detecciones de una anomalía en la Red de Telecomunicaciones.			
33	Se comprueba que los equipos inalámbricos son gestionados de forma segura y confiable, considerando para ello la configuración de los equipos, controles de acceso y configuración de seguridad.			

Fuente: (El Autor, 2018)

Las métricas establecidas por el equipo del proyecto para el aseguramiento de la calidad de los entregables, son las siguientes:

Cuadro No. 32: Métricas de Calidad del Proyecto

Objetivo de Calidad	Métrica (s)	Definición de la métrica	Resultado esperado	Frecuencia de medición	Responsable
Cumplimiento Normativo	Normas técnicas para la gestión y el control de las Tecnologías de Información. Acuerdo SUGEF 14-17	Cumplimiento de los lineamientos establecidos en el Marco Normativo Costarricense	Inscripción de la Firma EEQA en el registro de oferentes de la SUGEF	Semanal	Equipo de Auditores
Plan de Gestión	COBIT ITIL ISO-27001	Aplicar las mejores prácticas que suministran los marcos de referencia COBIT e ITIL, así como el estándar ISO-27001	Incremento de las posibilidades de obtener los resultados trazados con el desarrollo del proyecto	Semanal	Director del Proyecto
Requisitos del Proyecto	SPI – Schedule performance index acumulado	Gestión de valor ganado	SPI > 0.9	Mensual	Director del Proyecto
Requisitos del Proyecto	CPI – Cost Performance Index acumulado	Gestión de valor ganado	CPI > 0.9	Mensual	Director del Proyecto
Requisitos del Proyecto	+- 20% de holgura en el tiempo	No se podrá desviar el tiempo en más de 5 días.	Garantizar que el proyecto finalice dentro del tiempo pactado	Semanal	Director del Proyecto
Requisitos del Proyecto	+- 5% de holgura en el presupuesto	No se podrá variar el presupuesto en más o menos del 5% del monto establecido	Garantizar que el costo del proyecto sea el presupuestado desde el inicio, ver acta del proyecto.	Semanal	Director del Proyecto
Diseño de la Propuesta de Auditoría	Conformando por 3 principales áreas de revisión	Considerar la revisión de equipo de telecomunicaciones, servidores y bases de datos.	Abarcar la revisión del 100% de los recursos tecnológicos críticos de la organización.	Diario	Asesor Tecnológico
Herramienta para la Valoración de Riesgos de TI	Considera valores cualitativos y cuantitativos	Con base en los conceptos de probabilidad e impacto.	Identificación de riesgos de orden tecnológico.	Quincenal	Equipo de Auditores

Fuente: (El Autor, 2018)

En lo referente al plan de mejora continua, se establece el siguiente procedimiento para la toma de acciones preventivas y correctivas en el proyecto:

Cuadro No. 33: Proceso para la Toma de Acciones Preventivas o Correctivas

Paso	Responsable
1. Identificación de una problemática existente en el proyecto.	Equipo de proyecto
2. Evaluación por parte del Director del Proyecto o de los Socios de la Firma EEQA, para definir la importancia o nivel de la prioridad a asignarse a dicha problemática para su atención.	Director del Proyecto
3. Aprobación y asignación de recursos para el desarrollo de la acción correctiva o preventiva identificada.	Consejo Asesor de Cambios (CAB)
4. Sesión de trabajo para identificación de causas y soluciones a la problemática planteada.	Director del Proyecto
5. Identificación de la causa raíz y lluvia de ideas para determinar acciones correctivas y/o preventivas.	Director del Proyecto
6. Desarrollo de la propuesta de acción correctiva o preventiva.	Equipo de trabajo
7. Aprobación de la propuesta de acción correctiva o preventiva.	Consejo Asesor de Cambios (CAB)
8. Comunicación, implementación y registro documental de acción correctiva o preventiva aprobada.	Director del Proyecto

Fuente: (El Autor, 2018)

4.6 Plan de Gestión de los Recursos Humanos

La gestión de los recursos humanos toma en consideración los procesos que organizan, gestionan y conducen al equipo del proyecto, con la finalidad de reclutar personas con competencias idóneas y debidamente capacitadas para asumir los roles y las responsabilidades circunscritas al proyecto, donde valores tales como la participación y la sinergia son fundamentales.

Por consiguiente, una vez analizados los requerimientos del proyecto, se detalla el equipo necesario para su implementación, a través del siguiente organigrama:

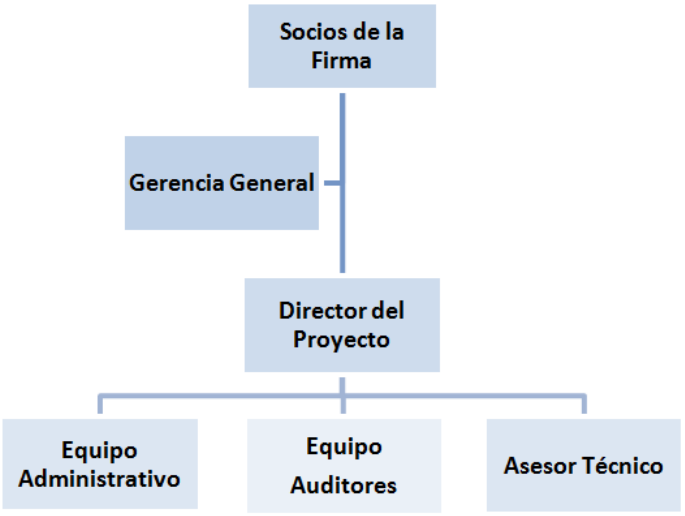


Figura No. 9. Organigrama del Proyecto
Fuente: (El Autor, 2018)

Los principales roles y responsabilidades del equipo de trabajo para el desarrollo de la propuesta para auditar un sistema de gestión de seguridad de la información, son:

• Socios de la Firma: Además de plantear el Plan Estratégico para la Firma EEQA, proporcionarán los recursos necesarios para el desarrollo e implementación del proyecto, de conformidad con el rol de patrocinador.

• Gerencia General: En el caso del presente proyecto, se encargará de brindar seguimiento al desarrollo del proyecto y proporcionará apoyo para identificar desviaciones a la línea base establecida.

• Director del Proyecto: Encargado de organizar y velar porque se cumplan cada una de las actividades acordadas para la completar la entrega del producto final.

• Equipo de Auditores: Responsable de definir los requerimientos desde la perspectiva de auditoría

• Equipo Administrativo: Proporciona los procesos administrativos requeridos para la ejecución del proyecto, como lo son las adquisiciones y la coordinación de capacitaciones.

• Asesor Técnico: Experto en el tema de seguridad informática, brinda la consultoría necesaria para desarrollar un plan de revisión que considere la aplicación de herramientas tecnológicas para la identificación de vulnerabilidades y brechas de seguridad.

Cuadro No. 34: Matriz de Roles y Responsabilidades

Matriz de Roles y Responsabilidades		Recursos					
EDT	**Actividad**	**Patrocinador (Socios de la**	**Gerencia General**	**Director del Proyecto**	**Equipo Administrativ**	**Equipo de Auditores**	**Asesor Técnico**
1.1	Identificación de Requisitos del Proyecto	A	I	R	C	C	C
1.1.1	Reunión con la Firma de Consultoría EEQA	A	I	R	C	C	C
1.1.1.1	Levantamiento de Requisitos Generales del Proyecto	A	I	R	C	C	C
1.1.1.2	Levantamiento de Requisitos Técnicos del Proyecto	A	I	R	C	C	C
1.2	**Especificación del Marco Normativo**	I	I	A	I	R	C
1.2.1	Legislación Costarricense	I	I	A	I	R	C
1.2.1.1	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR	I	I	A	I	R	C
1.2.1.2	Acuerdo SUGEF 14-17	I	I	A	I	R	C
1.2.2	Estándares y Marcos de Referencia Internacionales	I	I	A	I	R	C
1.2.2.1	COBIT – ISACA	I	I	A	I	R	C
1.2.2.2	ITIL	I	I	A	I	R	C
1.2.2.3	ISO-27001	I	I	A	I	R	C
1.2.2.4	Punto de Control No.1: Revisión de los Requerimientos	A	I	R	I	C	I

Matriz de Roles y Responsabilidades		Recursos					
EDT	**Actividad**	**Patrocinador (Socios de la**	**Gerencia General**	**Director del Proyecto**	**Equipo Administrativ**	**Equipo de Auditores**	**Asesor Técnico**
	y del Marco Normativo Aplicable						
1.3	**Implementación de Herramientas Tecnológicas**	I	I	A	I	R	C
1.3.1	Herramientas para el Análisis de Datos	I	I	A	I	R	C
1.3.1.1	Análisis de viabilidad para la instalación de la herramienta “ACL”	I	I	A	I	R	C
1.3.1.2	Análisis de viabilidad para la instalación de la herramienta “IDEA”	I	I	A	I	R	C
1.3.1.3	Análisis de viabilidad para la instalación de la herramienta “TOAD”	I	I	A	I	R	C
1.3.2	Herramientas para el Escaneo de Vulnerabilidades	I	I	A	I	C	R
1.3.2.1	Estudio de herramientas para escaneo de vulnerabilidades en Servidores	I	I	A	I	C	R
1.3.2.2	Estudio de herramientas para escaneo de vulnerabilidades en Redes	I	I	A	I	C	R
1.3.2.3	Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos	I	I	A	I	C	R

Matriz de Roles y Responsabilidades		Recursos					
EDT	**Actividad**	**Patrocinador (Socios de la**	**Gerencia General**	**Director del Proyecto**	**Equipo Administrativ**	**Equipo de Auditores**	**Asesor Técnico**
1.3.2.4	Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Implementar	A	I	R	I	C	C
1.4	**Elaboración y formalización de procedimientos de Auditoría**	A	I	A	I	R	C
1.4.1	Elaboración de Políticas	A	I	A	I	R	C
1.4.2	Elaboración de Procedimientos	A	I	A	I	R	C
1.4.3	Elaboración de Instructivos y Manuales	A	I	A	I	R	C
1.4.4	Punto de Control No.3: Evaluación de los Procedimientos de Auditoría	A	I	R	I	C	I
1.5	**Definición de Herramienta para la Valoración de Riesgos de TI**	I	I	A	I	R	C
1.5.1	Matriz SEVRI de la Contraloría General de la República	I	I	A	I	R	C
1.5.2	RISK IT de ISACA	I	I	A	I	R	C
1.5.3	MARGERIT	I	I	A	I	R	C
1.5.4	AS/NZS	I	I	A	I	R	C
1.6	**Gestión del Recurso Humano**	I	I	A	R	C	C
1.6.1	Definición del Perfil del Personal de Auditoría de TI	I	I	A	R	C	C
1.6.2	Capacitación del Personal	I	I	A	R	C	C

Matriz de Roles y Responsabilidades		Recursos					
EDT	**Actividad**	**Patrocinador (Socios de la**	**Gerencia General**	**Director del Proyecto**	**Equipo Administrativ**	**Equipo de Auditores**	**Asesor Técnico**
1.7	**Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad**	I	I	A	I	C	R
1.7.1	Seguridad de las Aplicaciones	I	I	A	I	C	R
1.7.2	Seguridad de la Información	I	I	A	I	C	R
1.7.3	Seguridad de la Infraestructura	I	I	A	I	C	R
1.7.4	Seguridad de la Gestión del Recurso Humano	I	I	A	I	C	R
1.7.5	Punto de Control No.4: Evaluación del Plan para la Revisión del SGSI	A	I	R	I	I	C
1.8	**Entrega del Proyecto**	A	I	R	C	C	I
1.8.1	Firma de Aceptación de los Entregables del Proyecto	A	I	R	C	C	I
1.8.2	Facturación del Proyecto	A	I	R	C	C	I
1.8.3	Documentos del Proyecto	A	I	R	C	C	I
1.8.3.1	Documentación de las Lecciones Aprendidas	A	I	R	C	C	I
1.8.4	Cierre de Adquisiciones	A	I	R	C	C	I
R: Responsable A: Autoriza C: Consultado I: Informado							

Fuente: (El Autor, 2018)

En cuanto al calendario de los recursos, en los cuadros No. 22 y No. 23 respectivamente, se consigna cuándo serán requeridos los miembros del equipo del proyecto para cada una de las actividades planificadas.

4.7 Plan de Gestión del Riesgo

La Gestión de los Riesgos del Proyecto *"incluye los procesos para llevar a cabo la planificación de la gestión de riesgos, así como la identificación, análisis, planificación de respuesta y control de los riesgos de un proyecto."* (PMI, 2013, pág. 309). Básicamente, se busca aumentar la probabilidad y el impacto de los eventos positivos en el proyecto, a la vez que se disminuye la probabilidad y el impacto de los eventos negativos.

Para la registrar los riesgos existentes en el proyecto, el equipo de trabajo aplicó como técnicas o herramientas de identificación de riesgos, la revisión de la documentación y una variante de la técnica de Delphi. De esta forma se puede consultar dicho registro en el momento que el proyecto lo requiera, así como planificar la respuesta al riesgo acorde a su categorización y priorización.

A continuación, se describen cada uno de los campos que conforman el listado unificado de los riesgos proyecto.

- **Código identificador del riesgo:** El código de identificación permite trabajar de forma estandarizada y ser incluido en una base de datos de riesgos. Este va a tener la estructura RX-YY-ZZ, donde ZZ es un consecutivo, YY representa el segundo nivel de la RBS y la "X" es la Categoría del Riesgo:

  RA- Riesgo de Administración de Proyectos
  RE- Riesgo Externo
  RO- Riesgo Organizacional
  RT- Riesgo Técnico

- **Causa del riesgo:** Se indica el primer nivel, segundo nivel y tercer nivel (si aplica) para cada uno de los riesgos identificados, siendo la causa el nivel más bajo de la RBS.

- **Descripción del riesgo:** SI **<evento o condición de incertidumbre>** debido a **<causas>** puede **<impacto positivo o negativo> <objetivos del proyecto>**

- **Referencia:** Lugar en un documento, requerimiento u otra seña que indique donde fueron encontrados los riesgos.

- **WBS:** En caso que el riesgo afecte un paquete de actividades específico del proyecto se indicará en esta columna.

Cuadro No. 35: Matriz de Registro de Riesgos del Proyecto

No	Código	Causa	Descripción del Riesgo	Referencia	WBS
01	RT-1.1-01	Técnico-Requisitos	Si no se encuentran bien definidos los requerimientos, las especificaciones técnicas y el alcance de la propuesta de Auditoría a implementar, se podrían presentar retrasos en el desarrollo de la misma, re-trabajo por la necesidad de replantear los requerimientos lo que consume más tiempo y recursos y que no se logren resolver las necesidades de los clientes que eventualmente contraten a la Firma EEQA.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	1.1

02	RT-1.3-01	Técnico-Complejidad	Si la complejidad técnica del software y hardware empleado como en el desarrollo de las auditorías no satisfacen las necesidades establecidas por los clientes o no se utiliza apropiadamente por el equipo de auditores, se podría ver afectada la ejecución de la auditoría, entre otras razones por la recolección de evidencia que no permite brindar recomendaciones objetivas, oportunas y objetivas.	Documentos de la Gestión de Adquisiciones	1.3
03	RT-1.4-01	Técnico-Capacitación	Si la Firma EEQA no implementa una estrategia para capacitar a su personal y transferir el conocimiento, se podría incurrir en dependencia tecnológica sobre proveedores, afectando variables como el costo operativo, eficiencia y demoras para identificar problemas.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	1.4
04	RE-2.1-01	Externo-Proveedores-Contratos	Si la revisión de aspectos consignados en los contratos suscritos con los clientes y proveedores, no es efectuado minuciosamente, lo que puede repercutir que el plan de auditoría no cubra las necesidades del cliente y se generen litigios por incumplimiento de acuerdos o contratos.	Contratos	2.1
05	RE-2.1-02	Externo-Proveedores-Contratos	Si se produce exposición, divulgación o fuga de información confidencial tanto del cliente como de la Firma EEQA, se puede materializar la pérdida de activos y consecuencias financieras, pérdida de imagen empresarial y la utilización de la información de los clientes por parte de los proveedores de manera indebida. Pérdida de compromiso legal del cliente o del proveedor.	Acuerdos de Confidencialidad	2.1
06	RE-2.1-03	Externo-Proveedores-Calidad de la Asesoría	Si existen debilidades de fondo en la propuesta de auditoría debido a recomendaciones de baja calidad emitidas por los proveedores tecnológicos y de seguridad, se puede afectar negativamente los entregables finales y objetivos propuestos con el desarrollo del proyecto y que el cliente meta no adquiera los servicios de la firma.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	2.1

07	RE-2.1-04	Externo-Proveedores-Fallas Técnicas	Se los proveedores tecnológicos de la Firma EEQA incumplen con la entrega de las herramientas requeridas para auditar un SGSI, o dichas herramientas no funcionan según lo indicado, puede retrasarse el proyecto y que no se entregue los servicios de asesoría de calidad o bajo un tiempo de respuesta inapropiado.	Contratos	2.1
08	RE-2.2-01	Externo-Regulatorio-	Si se presentan variaciones en el contexto (Política Pública de restricción del gasto, marco normativo costarricense, etc), la Firma EEQA podría resultar no se contratada por entidades principalmente del sector público.	Estudios de Factibilidad, Análisis de Riesgos	2.2
09	RE-2.2-02	Externo-Regulatorio-Permisos	Si existe incumplimiento de las obligaciones regulatorias y legales de conformidad con la normativa establecida, podría no recibirse la autorización para inscribirse como proveedor de servicios de auditoria ante la SUGEF.	Marco Normativo Costarricense	2.2
10	RE-2.3-01	Externo-Competencia	Si los servicios proporcionados por las firma consultoras que compiten con EEQA, presentan mayor valor agregado para el mercado meta, podría ser que el producto presentado por la firma EEQA no se logre desarrollar y se deba descontinuar la entrega del servicio.	Estudios de Factibilidad	2.3
11	RE-2.4-01	Externo-Cliente-Solicitud de Servicios	Si una vez desarrollada la propuesta de auditoría no alcanza la aceptación esperada entre los clientes de la firma al ser comercializada, se puede no lograr la rentabilidad esperada ocasionando daños a la imagen empresarial.	Lecciones aprendidas	2.4
12	RO-3.1-01	Organizacional-Dependencias del Proyecto-Coordinación y Logística.	Si el personal de la Firma EEQA no se involucra eficazmente en la generación del “Plan de Revisión de los Recursos de TI”, desde la perspectiva de seguridad y dicha actividad recae únicamente en el Asesor de Seguridad Informática, se podría presentar generar una dependencia crítica para el proyecto, en la figura del consultor externo contratado.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	3.1

13	RO-3.2-01	Organizacional-Recursos-Desempeño	Si existe carencia de conocimiento en el Recurso Humano que se encargará de la ejecución de las auditorias en tecnologías de información o en su defecto, una vez capacitado se genera la fuga de personal especializado debido principalmente a nuevas oportunidades laborales, podría presentarse que el desempeño del personal que deba asumir las funciones de auditoría no sea acorde con las normas de calidad establecidas en la Firma EEQA.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	3.2
14	RO-3.3-01	Organizacional-Financiación-Presupuesto	Si se utiliza información obsoleta y no se consideran todos los costos asociados para el desarrollo del proyecto, se puede incurrir en una definición errónea del financiamiento requerido para su implementación.	Documentos de la Gestión de Adquisiciones.	3.3
15	RO-3.4-01	Organizacional-Priorización	Si los Socios de la Firma EEQA modifican su Plan Estratégico, podrían ser reubicados los recursos empleados en el presente proyecto y desarrollarse otros productos de auditoría o consultoría.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	3.4
16	RA-4.1-01	Dirección de Proyectos - Estimación	Si se hace necesario adquirir más recursos de los planeados por errores en la estimación, se incrementará el costo del proyecto.	Presupuesto del proyecto	4.1
17	RA-4.2-01	Dirección de Proyectos-Planificación	Si no hay entendimiento de los objetivos y requerimientos del proyecto, se puede incurrir en una planificación ineficiente de los recursos lo que desemboca en un proyecto diseñado de forma inadecuada e incumplimiento de los criterios de la gestión de proyectos (tiempo, costo y calidad).	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	4.2
18	RA-4.2-02	Dirección de Proyectos-Planificación-Recursos humanos	Si los recursos humanos para el proyecto no son suficientes por errores en la planificación se puede afectar la calidad final del plan de auditoría.	Plan para la Dirección del Proyecto, Plan de Gestión de Recursos Humanos	4.2
19	RA-4.2-03	Dirección de Proyectos-Planificación-Recursos Humanos	Si los roles y responsabilidades del equipo encargado del desarrollo e implementación del plan de auditoría, no se establecen y distribuyen oportunamente y de forma eficaz, por fallas en la gestión de recursos humanos, se podría afectar la implementación y ejecución de las auditorías.	Plan para la Dirección del Proyecto, Cronograma de Actividades, Plan de Gestión de Recursos Humanos	4.2
20	RA-4.2-04	Dirección de Proyectos-Planificación - Adquisiciones	Si no se verifica que los proveedores cumplen con sus obligaciones tributarias como lo son la CCSS y Fodesaf, por falla en la gestión de adquisiciones, se podría presentar incumplimientos en el alcance, tiempo y presupuesto del proyecto.	Documentos de la Gestión de Adquisiciones.	4.2

21	RA-4.2-05	Dirección de Proyectos-Planificación - Adquisiciones	Si los requisitos técnicos del hardware y software e implementos requeridos no se definieron dentro de la planeación de necesidades, se puede afectar el presupuesto del proyecto.	Plan de Dirección del proyecto, Presupuesto del proyecto	4.2
22	RA-4.3-01	Dirección de Proyectos-Control-Cronograma	Si el control del proyecto no es suficiente por falta de seguimiento a la ejecución puede afectar el cronograma, el costo, el alcance y la calidad del proyecto.	Plan para la Dirección del Proyecto	4.3
23	RA-4.3-02	Dirección de Proyectos-Control-Cambios	Si los cambios del proyecto no se realizan de conformidad con los procedimientos formalizados, podría ocurrir que las actividades o procesos del proyecto se ejecuten sin la debida autorización, generando inconsistencias y errores en la ejecución.	Procedimiento para la Aplicación de Cambios	4.3
24	RA-4.4-01	Dirección de Proyectos-Comunicación-Medios y Canales	Si los medios y canales de comunicación no se establecen adecuadamente, la implementación y ejecución de la actividad podrían no efectuarse acorde a los requerimientos establecidos.	Plan de Gestión de la Comunicación	4.4
25	RA-4.4-02	Dirección de Proyectos-Comunicación-Medios y Canales	Si hay falta de comunicación entre el Asesor de Seguridad Informática y el personal de la Firma EEQA, se podría generar que el Plan de Trabajo de Seguridad de TI no sea asimilado adecuadamente por el personal que deberá ejecutarlo o que existan dudas en la realización de ciertas tareas.	Plan de Gestión de la Comunicación	4.4

Fuente: (El Autor, 2018)

Una estructura de desglose de riesgos (RBS) es un instrumento de considerable utilidad para especificar las distintas fuentes que pueden dar origen a un riesgo dentro del proyecto, ya que representa jerárquicamente los riesgos según sus categorías. En la siguiente figura se muestra la RBS desarrollada, de acuerdo con las categorías de segundo y tercer nivel que pudieron ser identificadas con el listado de riesgos.

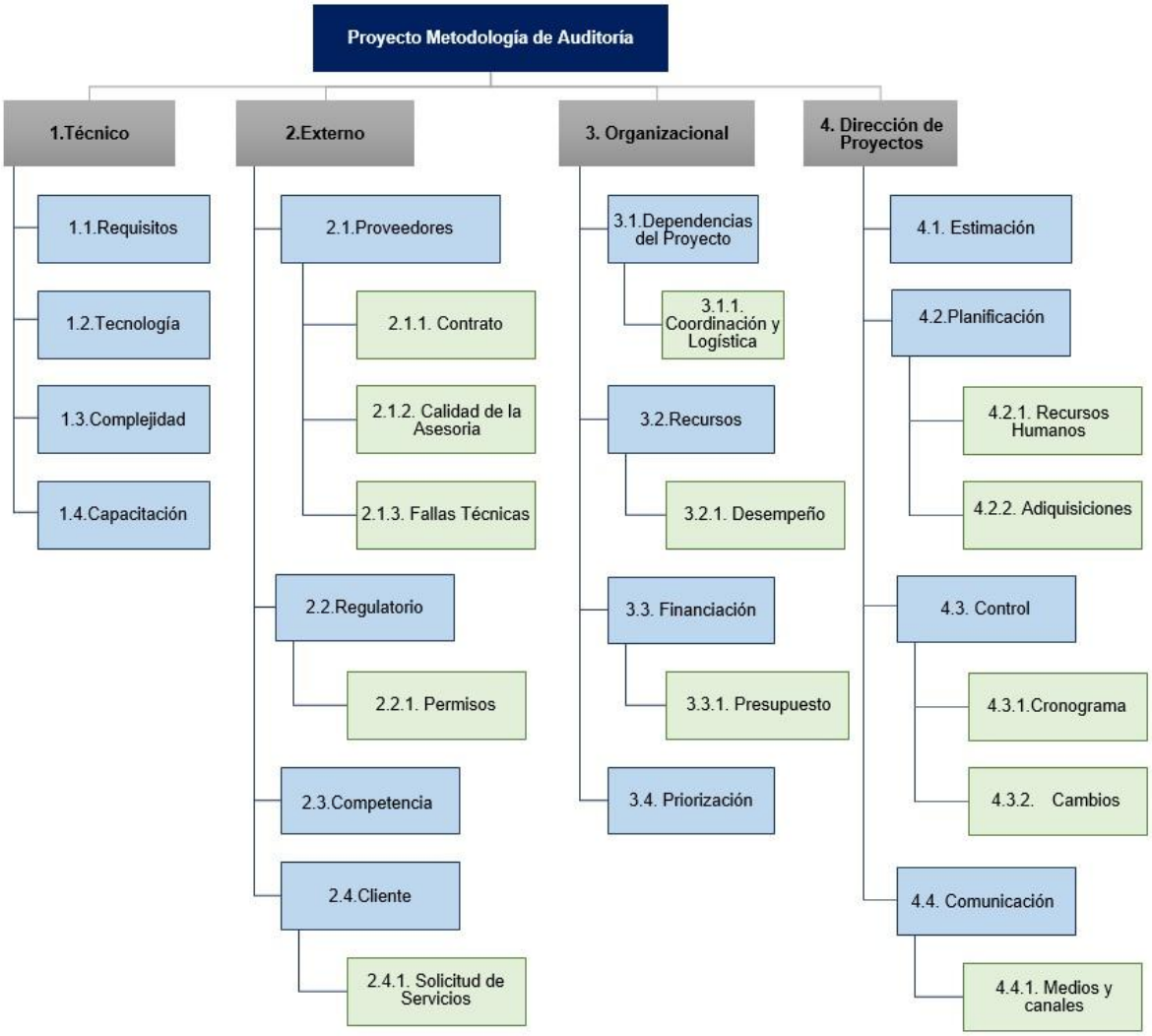


Figura No. 10. Estructura de Desglose de Riesgos del Proyecto

Fuente: (El Autor, 2018)

Posterior a la identificación de los riesgos, se procede a categorizar y priorizar cada uno de ellos, aplicando los conceptos de “Impacto” y “Probabilidad”, de conformidad con las siguientes escalas establecidas. Como resultado se obtiene el “Riesgo Inherente”.

Cuadro No. 36: Escala de Probabilidad del Riesgo

No.	Valor Cualitativo	Valor Cuantitativo
1	Muy Probable	0.9
2	Bastante Probable	0.7
3	Probable	0.5
4	Poco Probable	0.3
5	Muy Poco Probable	0.1

Fuente: (El Autor, 2018)

Cuadro No. 37: Escala de Impacto del Riesgo

Objetivo del Proyecto	Muy Bajo (.05)	Bajo (.1)	Moderado (.2)	Alto (.4)	Muy Alto (.8)
Costo	Insignificante incremento del costo	Incremento del costo < 1.5%	Incremento del costo entre el 1.5 – 3 %	Incremento del costo entre el 3 – 5 %	Incremento del costo > 5 %
Cronograma	Insignificante variación del calendario	variación del calendario < 1.5%	Desviación general del Proyecto 1.5 – 3 %	Desviación general del Proyecto 3 – 5 %	Desviación general del Proyecto > 5 %
Alcance	Reducción del alcance apenas perceptible	Áreas menores del alcance son afectadas	Áreas mayores del alcance son afectadas	Reducción del alcance inaceptable para el cliente	El producto final del proyecto es inservible
Calidad	Degradación de la calidad apenas perceptible	Solo aplicaciones muy específicas son afectadas	La reducción de la calidad demanda la aprobación del cliente	Reducción de la calidad inaceptable para el cliente	El producto final del proyecto es inservible

Fuente: (PMI, 2013)

Cuadro No. 38: Matriz de Probabilidad por Impacto

Impacto X Probabilidad	Muy Bajo (.05)	Bajo (.1)	Moderado (.2)	Alto (.4)	Muy Alto (.8)
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08

Fuente: (PMI, 2013)

A continuación, se procede con el análisis de priorización de riesgos, acorde con el instrumento antes detallado:

Cuadro No. 39: Matriz de Priorización del Riesgo

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
RT-1.1-01	Si no se encuentran bien definidos los requerimientos, las especificaciones técnicas y el alcance de la propuesta de Auditoría a implementar, se podrían presentar retrasos en el desarrollo de la misma, re-trabajo por la necesidad de replantear los requerimientos lo que consume más tiempo y recursos y que no se logren resolver las necesidades de	0.5	0.8	**0.40**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	los clientes que eventualmente contraten a la Firma EEQA.			
RT-1.3-01	Si la complejidad técnica del software y hardware empleado como en el desarrollo de las auditorías no satisfacen las necesidades establecidas por los clientes o no se utiliza apropiadamente por el equipo de auditores, se podría ver afectada la ejecución de la auditoría, entre otras razones por la recolección de evidencia que no permite brindar recomendaciones objetivas, oportunas y objetivas.	0.5	0.4	**0.20**
RT-1.4-01	Si la Firma EEQA no implementa una estrategia para capacitar a su personal y transferir el conocimiento, se podría incurrir en dependencia tecnológica sobre proveedores, afectando variables como el costo operativo, eficiencia y demoras para identificar problemas.	0.5	0.8	**0.40**
RE-2.1-01	Si la revisión de aspectos	0.5	0.4	**0.20**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	consignados en los contratos suscritos con los clientes y proveedores, no es efectuado minuciosamente, lo que puede repercutir que el plan de auditoría no cubra las necesidades del cliente y se generen litigios por incumplimiento de acuerdos o contratos.			
RE-2.1-02	Si se produce exposición, divulgación o fuga de información confidencial tanto del cliente como de la Firma EEQA, se puede materializar la pérdida de activos y consecuencias financieras, pérdida de imagen empresarial y la utilización de la información de los clientes por parte de los proveedores de manera indebida. Pérdida de compromiso legal del cliente o del proveedor.	0.3	0.8	**0.24**
RE-2.1-03	Si existen debilidades de fondo en la propuesta de auditoría debido a recomendaciones de baja calidad emitidas por los proveedores tecnológicos y de	0.3	0.8	**0.24**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	seguridad, se puede afectar negativamente los entregables finales y objetivos propuestos con el desarrollo del proyecto y que el cliente meta no adquiera los servicios de la firma.			
RE-2.1-04	Se los proveedores tecnológicos de la Firma EEQA incumplen con la entrega de las herramientas requeridas para auditar un SGSI, o dichas herramientas no funcionan según lo indicado, puede retrasarse el proyecto y que no se entregue los servicios de asesoría de calidad o bajo un tiempo de respuesta inapropiado.	0.5	0.8	**0.40**
RE-2.2-01	Si se presentan variaciones en el contexto (Política Pública de restricción del gasto, marco normativo costarricense, etc), la Firma EEQA podría resultar no se contratada por entidades principalmente del sector público.	0.3	0.8	**0.24**
RE-2.2-02	Si existe incumplimiento de las obligaciones regulatorias y	0.3	0.8	**0.24**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	legales de conformidad con la normativa establecida, podría no recibirse la autorización para inscribirse como proveedor de servicios de auditoría ante la SUGEF.			
RE-2.3-01	Si los servicios proporcionados por las firma consultoras que compiten con EEQA, presentan mayor valor agregado para el mercado meta, podría ser que el producto presentado por la firma EEQA no se logre desarrollar y se deba descontinuar la entrega del servicio.	0.5	0.4	**0.20**
RE-2.4-01	Si una vez desarrollada la propuesta de auditoría no alcanza la aceptación esperada entre los clientes de la firma al ser comercializada, se puede no lograr la rentabilidad esperada ocasionando daños a la imagen empresarial.	0.3	0.8	**0.24**
RO-3.2-01	Si existe carencia de conocimiento en el Recurso Humano que se encargará de la ejecución de las auditorias	0.5	0.4	**0.20**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	en tecnologías de información o en su defecto, una vez capacitado se genera la fuga de personal especializado debido principalmente a nuevas oportunidades laborales, podría presentarse que el desempeño del personal que deba asumir las funciones de auditoría no sea acorde con las normas de calidad establecidas en la Firma EEQA.			
RO-3.4-01	Si los Socios de la Firma EEQA modifican su Plan Estratégico, podrían ser reubicados los recursos empleados en el presente proyecto y desarrollarse otros productos de auditoría o consultoría.	0.3	0.8	**0.24**
RA-4.1-01	Si se hace necesario adquirir más recursos de los planeados por errores en la estimación, se incrementará el costo del proyecto.	0.5	0.4	**0.20**
RA-4.2-01	Si no hay entendimiento de los objetivos y requerimientos del proyecto, se puede incurrir en una planificación ineficiente	0.5	0.4	**0.20**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	de los recursos lo que desemboca en un proyecto diseñado de forma inadecuada e incumplimiento de los criterios de la gestión de proyectos (tiempo, costo y calidad).			
RA-4.2-02	Si los recursos humanos para el proyecto no son suficientes por errores en la planificación se puede afectar la calidad final del plan de auditoría.	0.5	0.4	**0.20**
RA-4.2-04	Si no se verifica que los proveedores cumplen con sus obligaciones tributarias como lo son la CCSS y Fodesaf, por falla en la gestión de adquisiciones, se podría presentar incumplimientos en el alcance, tiempo y presupuesto del proyecto.	0.3	0.8	**0.24**
RA-4.2-05	Si los requisitos técnicos del hardware y software e implementos requeridos no se definieron dentro de la planeación de necesidades, se puede afectar el presupuesto del proyecto.	0.5	0.4	**0.20**
RA-4.3-01	Si el control del proyecto no es suficiente por falta de	0.3	0.8	**0.24**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	seguimiento a la ejecución puede afectar el cronograma, el costo, el alcance y la calidad del proyecto.			
RO-3.1-01	Si el personal de la Firma EEQA no se involucra eficazmente en la generación del “Plan de Revisión de los Recursos de TI”, desde la perspectiva de seguridad y dicha actividad recae únicamente en el Asesor de Seguridad Informática, se podría presentar generar una dependencia crítica para el proyecto, en la figura del consultor externo contratado.	0.3	0.4	**0.12**
RO-3.3-01	Si se utiliza información obsoleta y no se consideran todos los costos asociados para el desarrollo del proyecto, se puede incurrir en una definición errónea del financiamiento requerido para su implementación.	0.3	0.4	**0.12**
RA-4.2-03	Si los roles y responsabilidades del equipo encargado del desarrollo e implementación del plan de auditoría, no se establecen y	0.5	0.2	**0.10**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	distribuyen oportunamente y de forma eficaz, por fallas en la gestión de recursos humanos, se podría afectar la implementación y ejecución de las auditorías.			
RA-4.3-02	Si los cambios del proyecto no se realizan de conformidad con los procedimientos formalizados, podría ocurrir que las actividades o procesos del proyecto se ejecuten sin la debida autorización, generando inconsistencias y errores en la ejecución.	0.3	0.4	**0.12**
RA-4.4-01	Si los medios y canales de comunicación no se establecen adecuadamente, la implementación y ejecución de la actividad podrían no efectuarse acorde a los requerimientos establecidos.	0.3	0.4	**0.12**
RA-4.4-02	Si hay falta de comunicación entre el Asesor de Seguridad Informática y el personal de la Firma EEQA, se podría generar que el Plan de Trabajo de Seguridad de TI no sea asimilado adecuadamente	0.3	0.4	**0.12**

Código	Descripción del Riesgo	Probabilidad	Impacto	Riesgo
	por el personal que deberá ejecutarlo o que existan dudas en la realización de ciertas tareas.			

Fuente: (El Autor, 2018)

Una vez que se ha desarrollado la priorización de los riesgos del proyecto, se definen las respuestas para gestionar cada uno de ellos, con la finalidad de minimizar su impacto y para obtener el nivel de riesgo residual. Las medidas para la administración del riesgo se enumeran a continuación:

Cuadro No. 40: Matriz de Respuesta al Riesgo

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
RT-1.1-01	Si no se encuentran bien definidos los requerimientos, las especificaciones técnicas y el alcance de la propuesta de auditoría a implementar, se podrían presentar retrasos en el desarrollo de la	**0.5 * 0.4 = 0.20**	**Estrategia: Mitigar** Revisión y reuniones periódicas con el personal involucrado, para la depuración de los requerimientos. Se cuenta con procedimiento para desarrollo de requerimientos y	Equipo de Auditores de la Firma

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	misma, re-trabajo por la necesidad de replantear los requerimientos lo que consume más tiempo y recursos y que no se logren resolver las necesidades de los clientes que eventualmente contraten a la Firma EEQA.		metodología de proyectos. Seguimiento de proyectos.	
RE-2.1-04	Si los proveedores tecnológicos de la Firma EEQA incumplen con la entrega de las herramientas requeridas para auditar un SGSI, o dichas herramientas no funcionan según lo planificado, puede retrasarse el proyecto y que no se entregue los servicios de	**0.5 * 0.4 = 0.20**	**Estrategia: Transferir** Contrato con multa a proveedor con cláusula sobre incumplimiento de requisitos. Como medidas de respaldo, se deben definir bien los requerimientos y criterios de aceptación del equipo; asimismo,	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	asesoría de calidad o bajo un tiempo de respuesta inapropiado.		elaborar una lista de proveedores alternos en capacidad de proporcionar oportunamente equipos e implementos requeridos, en caso de falla de los proveedores primarios.	
RT-1.3-01	Si la complejidad técnica del software y hardware empleado como en el desarrollo de las auditorías no satisfacen las necesidades establecidas por los clientes o no se utiliza apropiadamente por el equipo de auditores, se podría ver afectada la ejecución de la	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Se conforma un Comité que da seguimiento y control de acciones en relación al tema tecnológico, considerando la complejidad técnica de las soluciones requeridas por los clientes, así como la obsolescencia tecnológica, entre otros aspectos.	Asesor experto en Seguridad Informática

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	auditoría, entre otras razones por la recolección de evidencia que no permite brindar recomendaciones objetivas y oportunas.			
RT-1.4-01	Si la Firma EEQA no implementa una estrategia para capacitar a su personal y transferir el conocimiento, se podría incurrir en dependencia tecnológica sobre proveedores, afectando variables como el costo operativo, eficiencia y demoras para identificar problemas.	**0.1 * 0.8 = 0.08**	**Estrategia: Mitigar** Se incorpora el tema de capacitación durante el proceso de definición presupuestal de los proyectos. El área de Recursos Humano de la Firma EEQA se encuentra formulando un plan de capacitación de personal.	Encargada del Área de Gestión de Talento Humano
RE-2.1-01	Si la revisión de aspectos consignados en los	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** La Firma de	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	contratos suscritos con los clientes y proveedores, no es efectuado minuciosamente, lo que puede repercutir que el plan de auditoría no cubra las necesidades del cliente y se generen litigios por incumplimiento de acuerdos o contratos.		Consultoría EEQA, cuenta con un Asesor Legal que se encarga de la revisión de contratos. Se aprueba la contratación por servicios profesionales de un Asesor Tecnológico, para la revisión de los elementos técnicos consignados en los contratos.	
RE-2.1-02	Si se produce exposición, divulgación o fuga de información confidencial tanto del cliente como de la Firma EEQA, se puede materializar la pérdida de activos y consecuencias financieras, pérdida de imagen	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Ejecución de análisis de riesgos para identificar los elementos que comprometen la información. Utilización de roles y perfiles. Clasificación de la Información. Firma de acuerdos de	Equipo de Auditores de la Firma

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	empresarial y la utilización de la información de los clientes por parte de los proveedores de manera indebida. Pérdida de compromiso legal del cliente o del proveedor.		confidencialidad.	
RE-2.1-03	Si existen debilidades de fondo en la propuesta de auditoría debido a recomendaciones de baja calidad emitidas por los proveedores tecnológicos y de seguridad, se puede afectar negativamente los entregables finales y objetivos propuestos con el desarrollo del proyecto y que el cliente meta no	**0.1 * 0.8 = 0.08**	**Estrategia: Mitigar** Revisión y reuniones periódicas con el personal involucrado, para la depuración de los requerimientos para el desarrollo de la propuesta de Auditoría.	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	adquiera los servicios de la firma.			
RE-2.2-01	Si se presentan variaciones en el contexto (Política Pública de restricción del gasto, marco normativo costarricense, etc), la Firma EEQA podría no ser contratada por entidades principalmente del sector público.	**0.3 * 0.4 = 0.12**	**Estrategia: Aceptar** En caso que el riesgo se materialice, continuar con el proyecto de suscripción de un acuerdo con alguna Firma Consultora Internacional, para mejorar la competitividad de la empresa y expandir operaciones en otros países.	Socios de la Firma
RE-2.2-02	Si existe incumplimiento de las obligaciones regulatorias y legales de conformidad con la normativa establecida, podría no recibirse la	**0.1 * 0.8 = 0.08**	**Estrategia: Mitigar** Se realizan revisiones periódicas del contenido de los manuales de procedimientos. Utilización de la	Equipo de Auditores de la Firma

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	autorización para inscribirse como proveedor de servicios de auditoría ante la SUGEF.		Intranet y correo electrónico como medio de divulgación de normativa empresarial. Permanente revisión del cumplimiento de la normativa regulatoria.	
RE-2.3-01	Si los servicios proporcionados por las firma consultoras que compiten con EEQA, presentan mayor valor agregado para el mercado meta, podría ser que el producto presentado por la firma EEQA no se logre desarrollar y se deba descontinuar la entrega del servicio.	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Observación de los productos y servicios proporcionados por la competencia. Proceso de mejora continúa de los productos y servicios proporcionados por la Firma EEQA. Seguimiento mediante puntos de control de los proyectos y coordinación con	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
			los involucrados de TI y la contraparte usuaria. Utilización de la metodología de gestión de proyectos.	
RE-2.4-01	Si una vez desarrollada la propuesta de auditoría no alcanza la aceptación esperada entre los clientes de la firma al ser comercializada, se puede no lograr la rentabilidad esperada ocasionando daños a la imagen empresarial.	**0.1 * 0.8 = 0.08**	**Estrategia: Mitigar** Desarrollar planes para la comercialización de la propuesta de auditoría, de conformidad con estudios de mercado.	Gerente General de la Firma
RO-3.2-01	Si existe carencia de conocimiento en el Recurso Humano que se encargará de la ejecución de las auditorias en	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Subcontratación de personal. Capacitación de personal. Desarrollar plan de	Encargada del Área de Gestión de Talento Humano

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	tecnologías de información o en su defecto, una vez capacitado se genera la fuga de personal especializado debido principalmente a nuevas oportunidades laborales, podría presentarse que el desempeño del personal que deba asumir las funciones de auditoría no sea acorde con las normas de calidad establecidas en la Firma EEQA.		traslado del conocimiento y sucesión del personal.	
RO-3.4-01	Si los Socios de la Firma EEQA modifican su Plan Estratégico, podrían ser reubicados los recursos	**0.1 * 0.8 = 0.08**	**Estrategia: Aceptar** En caso que el riesgo se materialice, se dará seguimiento de los	Socios de la Firma

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	empleados en el presente proyecto y desarrollarse otros productos de auditoría o consultoría.		planes estratégicos y tácticos de la Firma EEQA, principalmente de aquellos temas relacionados con las Tecnologías de Información. Priorización de presupuesto para cubrir la operación. Solicitar los recursos requeridos por el proyecto, a través de las modificaciones presupuestarias, en caso de ser necesario.	
RA-4.1-01	Si se hace necesario adquirir más recursos de los planeados por errores en la estimación, se incrementará el costo del proyecto.	**0.3 * 0.4 = 0.12**	**Estrategia: Aceptar** Establecer una reserva para contingencias**.** En caso que el riesgo se materialice, buscar otras	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
			fuentes alternativas para financiar proyecto, por ejemplo, préstamos bancarios. En caso extremo, se analizaría modificar el alcance del proyecto.	
RA-4.2-01	Si no hay entendimiento de los objetivos y requerimientos del proyecto, se puede incurrir en una planificación ineficiente de los recursos lo que desemboca en un proyecto diseñado de forma inadecuada e incumplimiento de los criterios de la gestión de proyectos (tiempo, costo y calidad).	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Revisión y reuniones periódicas con el personal involucrado, para la depuración de los requerimientos, tanto interno como externo. Se cuenta con procedimiento para desarrollo de requerimientos y metodología de proyectos. Seguimiento de proyectos.	Director del Proyecto
RA-4.2-	Si los recursos	**0.3 * 0.4**	**Estrategia: Mitigar**	Director del

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
02	humanos para el proyecto no son suficientes por errores en la planificación se puede afectar la calidad final del plan de auditoría.	**= 0.12**	Asegurar que el proceso de planificar la gestión de los recursos humanos sea óptimo. Incluir la participación de un asesor de la gestión del Talento Humano, que brinde seguimiento al cumplimiento de las buenas prácticas para la administración del Recurso Humano del proyecto.	Proyecto
RA-4.2-03	Si los roles y responsabilidades del equipo encargado del desarrollo e implementación del plan de auditoría, no se establecen y distribuyen	**0.3 * 0.2 = 0.06**	**Estrategia: Mitigar** Garantizar que el proceso de Planificar los Recursos Humanos se realice adecuadamente.	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	oportunamente y de forma eficaz, por fallas en la gestión de recursos humanos, se podría afectar la implementación y ejecución de las auditorías.		Incluir la participación de un asesor de la gestión del Talento Humano, que brinde seguimiento al cumplimiento de las buenas prácticas para la administración del Recurso Humano del proyecto.	
RA-4.2-04	Si no se verifica que los proveedores cumplen con sus obligaciones tributarias como lo son la CCSS y Fodesaf, por falla en la gestión de adquisiciones, se podría presentar incumplimientos en el alcance, tiempo y presupuesto del proyecto.	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Especificación de los requerimientos técnicos y de servicios para las contrataciones. Solicitud de garantías sobre la ejecución del proyecto por parte del proveedor. Seguimiento de acuerdos de servicio. Identificación de proveedores	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
			alternos / externos.	
RA-4.2-05	Si los requisitos técnicos del hardware y software e implementos requeridos no se definieron dentro de la planeación de necesidades, se puede afectar el presupuesto del proyecto.	**0.3 * 0.4 = 0.12**	**Estrategia: Mitigar** Elaboración de estudios técnicos más específicos, que se ajusten a las necesidades de los clientes de la Firma EEQA.	Asesor experto en Seguridad Informática
RA-4.3-01	Si el control del proyecto no es suficiente por falta de seguimiento a la ejecución puede afectar el cronograma, el costo, el alcance y la calidad del proyecto.	**0.1 * 0.8 = 0.08**	**Estrategia: Mitigar** Garantizar que los procesos de seguimiento y control de las Gestiones de Tiempo, Alcance, Costo y Calidad sean excelentes. El Gerente General de la Firma EEQA, desempeñará el por de fiscalizador del proyecto, que	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
			brinde seguimiento a la gestión de las restricciones contrapuestas del proyecto, como lo son el alcance, costos y la calidad.	
RO-3.1-01	Si el personal de la Firma EEQA no se involucra eficazmente en la generación del "Plan de Revisión de los Recursos de TI", desde la perspectiva de seguridad y dicha actividad recae únicamente en el Asesor de Seguridad Informática, se podría generar una dependencia crítica para el proyecto, en la figura del consultor externo contratado.	**0.1 * 0.4 = 0.04**	**Estrategia: Mitigar** Rotación de funciones. Capacitación y nombramiento de funcionarios de respaldo. Documentación de los procedimientos. Definición de reuniones para garantizar espacios para la comunicación entre las partes, involucrar a las jefaturas en el desarrollo del proyecto. Seguimiento a la ejecución de los	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
			puntos de control establecidos en el cronograma.	
RO-3.3-01	Si se utiliza información obsoleta y no se consideran todos los costos asociados para el desarrollo del proyecto, se puede incurrir en una definición errónea del financiamiento requerido para su implementación.	**0.1 * 0.4 = 0.04**	**Estrategia: Mitigar** Para la definición de los costos se evalúa las diversas alternativas contemplando todos los elementos; a su vez, se definen los costos de los insumos para el despliegue de los diversos servicios y se procede a registrarlos.	Director del Proyecto
RA-4.3-02	Si los cambios del proyecto no se realizan de conformidad con los procedimientos formalizados, podría ocurrir que las actividades o procesos del proyecto se ejecuten sin la	**0.1 * 0.4 = 0.04**	**Estrategia: Mitigar** Los cambios propuestos serán evaluados y autorizados por el Consejo Asesor de Cambios (CAB), integrado por los Socios de la Firma EEQA, el Gerente	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	debida autorización, generando inconsistencias y errores en la ejecución.		de Auditoría y por el Director del Proyecto.	
RA-4.4-01	Si los medios y canales de comunicación no se establecen adecuadamente, la implementación y ejecución de la actividad podrían no efectuarse acorde a los requerimientos establecidos.	**0.1 * 0.4 = 0.04**	**Estrategia: Mitigar** Gestionar las Comunicaciones eficientemente. Reuniones periódicas para discutir los avances del proyecto. Existencia de espacios de retroalimentación entre el personal responsable de la implementación del proyecto, antes, durante y después de la actividad.	Director del Proyecto
RA-4.4-02	Si hay falta de comunicación entre el Asesor de Seguridad	**0.1 * 0.4 = 0.04**	**Estrategia: Mitigar** Formalizar los medios y canales	Director del Proyecto

Código	Descripción del Riesgo	Riesgo	Respuesta al Riesgo	Responsable
	Informática y el personal de la Firma EEQA, se podría generar que el Plan de Trabajo de Seguridad de TI no sea asimilado adecuadamente por el personal que deberá ejecutarlo o que existan dudas en la realización de ciertas tareas.		de comunicación a lo interno del proyecto, con la finalidad de optimizar el flujo de la información.	

Fuente: (El Autor, 2018)

4.8 Plan de Gestión de las Comunicaciones

La Gestión de las Comunicaciones del Proyecto *"incluye procesos requeridos para asegurar que la planificación, recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados."* (PMI, 2013, pág. 287).

Como en todo proyecto, la comunicación debe ser óptima entre todos los involucrados lo que proporciona mayor oportunidad de éxito para alcanzar los objetivos propuestos. Cabe destacar que para el presente proyecto se maneja un lenguaje altamente técnico, propio del campo de las tecnologías de información, por lo que la gestión de la comunicación es un elemento fundamental.

En ese sentido, el correo electrónico empresarial es uno de los principales medios a utilizar para el flujo de la información del proyecto; asimismo, tanto las comunicaciones escritas, minutas y la intranet, son medios válidos para mantener informados a los involucrados del proyecto.

La periodicidad de las reuniones es semanal, para ello el Director de Proyecto convocará formalmente y de forma anticipada a cada uno de los asistentes, remitiendo además el contenido del temario que será analizado durante la reunión; finalmente, todos los acuerdos alcanzados, aprobación de entregables, solicitudes de cambios, avances del proyecto y reportes de seguimiento y control, serán debidamente documentados. También se pueden realizar reuniones de acuerdo a los puntos de control establecidos en el cronograma de actividades del proyecto.

En caso que las comunicaciones de las minutas se realicen por medio de documento físico, estas para ser aprobadas deben contar con las firmas y fechas respectivas; asimismo, al emplear el correo electrónico los participantes de la reunión deberán remitir su aprobación respondiendo el correo de manera que se da por aceptada la minuta y se considerará como la firma y la fecha del correo; los correos electrónicos deben contener un resumen de los puntos tratados y los acuerdos tomados así como los responsables y fechas acordadas.

Para mantener informados a los involucrados y asegurar una comunicación efectiva, se desarrolla la siguiente matriz de comunicación del proyecto por actividad, recurso, frecuencia y método, estableciendo con ello la forma y medio a utilizar para comunicar los aspectos o insumos principales a los miembros del equipo del proyecto:

Cuadro No. 41: Matriz de Comunicación del Proyecto

Matriz de Comunicación				Responsabilidad del Interesado					
EDT	Actividad	Frecuencia	Medio	Patrocinador (Socios de la	Gerencia General	Director del Proyecto	Equipo Administrativo	Equipo de Auditores	Asesor Técnico
1.1	**Identificación de Requisitos del Proyecto**								
1.1.1	Reunión con la Firma de Consultoría EEQA	1	R	A	D	E	S	S	S
1.1.1.1	Levantamiento de Requisitos Generales del Proyecto	1	DE	A	D	E	S	S	S
1.1.1.2	Levantamiento de Requisitos Técnicos del Proyecto	1	DE	A	D	E	S	S	S
1.2	**Especificación del Marco Normativo**								
1.2.1	Legislación Costarricense	D	DE	D	D	E	D	A,E	S
1.2.1.1	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la CGR	D	DE	D	D	E	D	A,E	S
1.2.1.2	Acuerdo SUGEF 14-17	D	DE	D	D	E	D	A,E	S
1.2.2	Estándares y Marcos de Referencia Internacionales	D	DE	D	D	E	D	A,E	S
1.2.2.1	COBIT – ISACA	D	DE	D	D	E	D	A,E	S
1.2.2.2	ITIL	D	DE	D	D	E	D	A,E	S
1.2.2.3	ISO-27001	D	DE	D	D	E	D	A,E	S
1.2.2.4	Punto de Control No.1: Revisión de los Requerimientos y del Marco Normativo Aplicable.	D	DE	D	D	E	D	A,E	S
1.3	**Implementación de Herramientas Tecnológicas**								
1.3.1	Herramientas para el Análisis de Datos	D	DE	D	D	A	D	E	S
1.3.1.1	Análisis de viabilidad para la	D	DE	D	D	A	D	E	S

Matriz de Comunicación				Responsabilidad del Interesado					
EDT	Actividad	Frecuencia	Medio	Patrocinador (Socios de la	Gerencia General	Director del Proyecto	Equipo Administrativo	Equipo de Auditores	Asesor Técnico
	instalación de la herramienta “ACL”								
1.3.1.2	Análisis de viabilidad para la instalación de la herramienta “IDEA”	D	DE	D	D	A	D	E	S
1.3.1.3	Análisis de viabilidad para la instalación de la herramienta “TOAD”	D	DE	D	D	A	D	E	S
1.3.2	**Herramientas para el Escaneo de Vulnerabilidades**								
1.3.2.1	Estudio de herramientas para escaneo de vulnerabilidades en Servidores	D	DE	D	D	A	D	S	E
1.3.2.2	Estudio de herramientas para escaneo de vulnerabilidades en Redes	D	DE	D	D	A	D	S	E
1.3.2.3	Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos	D	DE	D	D	A	D	S	E
1.3.2.4	Punto de Control No.2: Evaluación de las Herramientas Tecnológicas a Implementar	D	DE	D	D	A	D	S	E
1.4	**Elaboración y formalización de procedimientos de Auditoría**								
1.4.1	Elaboración de Políticas	D	DE	A	D	A	D	E	S
1.4.2	Elaboración de Procedimientos	D	DE	A	D	A	D	E	S
1.4.3	Elaboración de Instructivos y Manuales	D	DE	A	D	A	D	E	S
1.4.4	Punto de Control No.3: Evaluación de los Procedimientos de Auditoría	D	DE	A	D	A	D	E	S
1.5	**Definición de Herramienta para la Valoración de Riesgos de TI**								
1.5.1	Matriz SEVRI de la Contraloría General de la República	D	DE	D	D	A	D	E	S

Matriz de Comunicación				Responsabilidad del Interesado					
EDT	**Actividad**	**Frecuencia**	**Medio**	**Patrocinador (Socios de la**	**Gerencia General**	**Director del Proyecto**	**Equipo Administrativo**	**Equipo de Auditores**	**Asesor Técnico**
1.5.2	RISK IT de ISACA	D	DE	D	D	A	D	E	S
1.5.3	MARGERIT	D	DE	D	D	A	D	E	S
1.5.4	AS/NZS	D	DE	D	D	A	D	E	S
1.6	**Gestión del Recurso Humano**								
1.6.1	Definición del Perfil del Personal de Auditoría de TI	D	R	D	D	A	E	S	S
1.6.2	Capacitación del Personal	D	DE	D	D	A	E	S	S
1.7	**Creación del Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad**								
1.7.1	Seguridad de las Aplicaciones	D	DE	D	D	A	D	S	E
1.7.2	Seguridad de la Información	D	DE	D	D	A	D	S	E
1.7.3	Seguridad de la Infraestructura	D	DE	D	D	A	D	S	E
1.7.4	Seguridad de la Gestión del Recurso Humano	D	DE	D	D	A	D	S	E
1.7.5	Punto de Control No.4: Evaluación del Plan para la Revisión del SGSI	D	DE	D	D	A	D	S	E
1.8	**Entrega del Proyecto**								
1.8.1	Firma de Aceptación de los Entregables del Proyecto	1	R	A	D	E	S	S	D
1.8.2	Facturación del Proyecto	1	R	A	D	E	S	S	D
1.8.3	Documentos del Proyecto	D	DE	A	D	E	S	S	D
1.8.3.1	Documentación de las Lecciones Aprendidas	1	DE	A	D	E	S	S	D
1.8.4	Cierre de Adquisiciones	1	DE	A	D	E	S	S	D

Aspecto	Término	Significado
Frecuencia	D	Diario
	SE	Semanal
	M	Mensual
	1	Única vez
Medio	DI	Documento Impreso

Matriz de Comunicación				Responsabilidad del Interesado					
EDT	Actividad	Frecuencia	Medio	Patrocinador (Socios de la	Gerencia General	Director del Proyecto	Equipo Administrativo	Equipo de Auditores	Asesor Técnico

	DE	Documento Electrónico
	C	Correo Electrónico
	R	Reunión
	VC	Video Conferencia
	MI	Mensaje de Instantáneo
Responsabilidad	A	Autoriza
	D	Destinatario
	E	Emisor
	S	Soporte
	V	Valida
	NA	No Aplica

.

Fuente: (El Autor, 2018)

Durante el año 2017, la Firma EEQA suscribió un contrato de servicios con un proveedor tecnológico, con la finalidad de adquirir la modalidad de “Almacenamiento como Servicio”. A través de dicho servicio se obtiene soluciones de almacenamiento acorde las necesidades particulares de la empresa de consultoría, así como la instalación, mantenimiento y continuidad operativa. En síntesis, la contratación incluye el alquiler mensual de infraestructura tecnológica de almacenamiento, lo que posibilita a la Firma EEQA abstraerse de la complejidad de factores como arquitectura, rendimiento y seguridad, de manera que se asegura el resguardo de información empresarial.

El servicio supracitado será empleado para el manejo de la información del proyecto, por lo que la misma se encontrará disponible para ser consultada en el momento que sea requerido por cualquier miembro del equipo de trabajo que se encuentre debidamente autorizado para ello.

En lo referente al envío de reportes del proyecto, se utilizará como base el cronograma de actividades, por lo que cada uno de los reportes se debe remitir durante días hábiles laborales, ya que no se consideró como parte del cronograma días feriados ni trabajos que debieran realizarse durante horario nocturno.

4.9 Plan de Gestión de las Adquisiciones

Se define como *"el proceso de documentar las decisiones de adquisiciones del proyecto, especificar el enfoque e identificar a los proveedores potenciales."* (PMI, 2013, pág. 358).

El plan de adquisiciones formulado por la Firma EEQA, inicia con el análisis denominado "Hacer o Comprar", el cual *"es una técnica general de gestión utilizada para determinar si un trabajo particular puede ser realizado de manera satisfactoria por el equipo del proyecto o debe ser adquirido de fuentes externas."* (PMI, 2013, pág. 365).

Por reglamentación interna de la Firma EEQA, la responsabilidad de las decisiones de que hacer o comprar varía dependiendo de la cuantía de la compra, siendo los Socios de la Firma la máxima autoridad; no obstante, una vez planteado el presupuesto requerido por el proyecto, el Director del Proyecto conjuntamente con el Gerente de Auditoría de la Firma EEQA, definieron la siguiente propuesta:

Cuadro No. 42: Análisis de Hacer - Comprar

Actividad	Hacer	Comprar	Justificación
Análisis del Marco Normativo Costarricense (Normas Técnicas para la Gestión y el Control de las TI, SUGEF 14-17, etc.)	X		A pesar que la Firma EEQA no dispone de ningún tecnólogo en su planilla, el equipo de auditores tiene conocimiento sobre el Marco Normativo Costarricense; asimismo, han existido invitaciones de parte de la CGR para recibir capacitación sobre las Normas Técnicas para la Gestión y el Control de las TI.
Análisis de los estándares y marcos de referencia internacionales, que son aplicables en el desarrollo de la propuesta de Auditoría (COBIT, ITIL, ISO-27001)	X		A pesar que la Firma EEQA no dispone de ningún tecnólogo en su planilla, el equipo de auditores tiene conocimiento del alcance de estos estándares y marcos de referencia. Únicamente se consultará al Asesor de Seguridad de TI en aspectos muy específicos, más no se le atribuye la responsabilidad del entregable.

Evaluación de la viabilidad de implementar herramientas para el análisis de datos (ACL, IDEA, TOAD)		X	La complejidad técnica de la tarea demanda que la misma sea ejecutada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.
Evaluación de la viabilidad de implementar herramientas para el escaneo de vulnerabilidades en Servidores (Microsoft, UNIX, LINUX)		X	La complejidad técnica de la tarea demanda que la misma sea ejecutada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.
Evaluación de la viabilidad de implementar herramientas para el escaneo de vulnerabilidades en Servidores (Microsoft, UNIX, LINUX)		X	La complejidad técnica de la tarea demanda que la misma sea ejecutada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.
Evaluación de la viabilidad de implementar herramientas para el escaneo de vulnerabilidades en Redes de Telecomunicaciones (Cisco, Juniper, Huawei, etc.)		X	La complejidad técnica de la tarea demanda que la misma sea ejecutada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.

Evaluación de la viabilidad de implementar herramientas para el escaneo de vulnerabilidades en Bases de Datos (Oracle, SQL Server, MySQL, etc.)		X	La complejidad técnica de la tarea demanda que la misma sea ejecutada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.
Elaboración de políticas, procedimientos, manuales e instructivos de auditoría.	X	X	Para completar esta actividad, se requiere tanto el aporte del personal interno de la Firma EEQA, como del Asesor experto en seguridad informática.
Implementación de una herramienta para el análisis de riesgos de tecnologías de información.	X	X	Para completar esta actividad, se requiere tanto el aporte del personal interno de la Firma EEQA, como del Asesor experto en seguridad informática, con la finalidad de profundizar en el análisis de riesgos desde la perspectiva de TI.
Definición del perfil del personal de a cargo de ejecutar las auditorías de TI, de conformidad con el plan a desarrollar.	X		Las competencias de la Encargada del Gestión de Talento Humano de la Firma EEQA, le habilitan el asumir esta actividad.

Diseñar el plan de capacitación del personal de la Firma EEQA, que participará en la ejecución de las auditorías de TI, de conformidad con el plan a desarrollar.	X		Las competencias de la Encargada del Gestión de Talento Humano de la Firma EEQA, le habilitan el asumir esta actividad.
Formulación del "Plan de Revisión de los Recursos de TI", lo cual incluye la evaluación de las aplicaciones, seguridad de la información, la infraestructura de TI y la gestión del recurso humano.		X	La complejidad técnica de la tarea demanda que la misma sea desarrollada por un recurso especializado, cuyo perfil en la actualidad no forma parte del equipo humano de la Firma EEQA.

Fuente: (El Autor, 2018)

En relación con los criterios de selección de proveedores, la Firma EEQA cuenta con un reglamento interno de compra, el cual es de aplicación obligatoria en la contratación del Asesor experto en seguridad informática. Dicha contratación será adjudicada a un solo proveedor, dada la integración necesaria de los requisitos del proyecto.

Cuadro No. 43: Criterios de Selección de Proveedores

Criterio	Peso %
Mejor Precio	50%
Tiempo de Entrega	10%
Experiencia del Proveedor	10%
Calidad del Producto o Servicio	10%

Garantía	10%
Seguridad Ocupacional y Ambiente	10%
Total de Puntos a Obtener	**100%**

Fuente: (El Autor, 2018)

Las ofertas admitidas se compararán y adjudicarán de acuerdo al sistema de puntajes definido, siendo la oferta seleccionada para su adjudicación la que logre el mayor puntaje y cumpla con lo requerido por la Firma EEQA; asimismo, el Director del Proyecto asumirá el rol de administrador del contrato quien validará el cumplimiento de las normas establecidas para los proveedores.

En lo que respecta al tipo de contrato y dada su importancia para proteger desde la perspectiva jurídica los intereses de la firma, se han definido los siguientes criterios:

Cuadro No. 44: Identificación de Tipo de Contrato

Artículo o Servicio	Criterio de Éxito o Descripción Técnica	Tipo de Contrato	Descripción del Tipo de Contrato
Asesoría en Seguridad Informática	Desarrollo de un "Plan de Revisión de los Recursos de TI", alineado con estándares y marcos de referencia sobre las buenas prácticas de la gestión de las	Contrato de Precio Fijo	Establece un precio total fijo para un producto o servicio definido que se va a prestar; asimismo, pueden consignar incentivos financieros por alcanzar o superar

Artículo o Servicio	Criterio de Éxito o Descripción Técnica	Tipo de Contrato	Descripción del Tipo de Contrato
	tecnologías de información; Asimismo, debe incorporar el uso de herramientas para la detección de vulnerabilidades, brechas de seguridad y análisis de datos.		objetivos específicos del proyecto, entre ellos las fechas de entrega programadas, los costos del proyecto y el desempeño técnico.
Kilometraje	Pago único de $100 otorgado exclusivamente al Director del Proyecto y al Asesor en el tema de seguridad informática, por cuanto son los únicos miembros del equipo del proyecto que corresponde a personal externo de la Firma EEQA. Las sesiones de trabajo se desarrollan en las oficinas de la		En este tipo de contrato, los compradores deben definir con exactitud el producto o los servicios que son objetos de la adquisición. Por su parte, los vendedores se encuentran obligados por ley a cumplir dichos contratos; de lo contrario, se exponen a sanciones en caso de incumplimiento.

Artículo o Servicio	Criterio de Éxito o Descripción Técnica	Tipo de Contrato	Descripción del Tipo de Contrato
	firma.		
Servicios de Telecomunicaciones (Internet)	Pago único de $50 otorgado exclusivamente al Director del Proyecto y al Asesor en el tema de seguridad informática, por cuanto son los únicos miembros del equipo del proyecto que corresponde a personal externo de la Firma EEQA.		En este tipo de contrato existe la posibilidad de modificar el alcance establecido, previo acuerdo financiero entre las partes involucradas.
Telefonía Celular	Pago único de $50 otorgado exclusivamente al Director del Proyecto y al Asesor en el tema de seguridad informática, por cuanto son los únicos miembros del equipo del proyecto que		

Artículo o Servicio	Criterio de Éxito o Descripción Técnica	Tipo de Contrato	Descripción del Tipo de Contrato
	corresponde a personal externo de la Firma EEQA.		

Fuente: (El Autor, 2018)

Posteriormente, con base en el tipo de contrato para efectuar las adquisiciones que ha sido definido por el equipo de dirección del proyecto, se desarrolla el plan de dichas adquisiciones, con el fin de poder darle seguimiento a los desembolsos en que se debe incurrir para completar convenientemente las actividades del proyecto.

Cuadro No. 45: Matriz de las Adquisiciones

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
Servicios de Telecomunicaciones (Internet)	Se suministra desde el levantamiento de los requerimientos del proyecto hasta la entrega formal	Compra Directa	19/02/2018	18/05/2018	$ 100
Telefonía Celular		Compra Directa			$ 100
Kilometraje		Compra Directa			$ 200

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
	del mismo.				
Informe de viabilidad sobre la implementación del marco de referencia COBIT	El entregable se desarrolla con la asesoría del experto en seguridad informática.	Compra Directa	22/02/2018	23/02/2018	$ 75
Curso de Fundamentos ITIL para la gestión de servicios de TI.	Capacitar al menos un recursos de la Firma EEQA, sobre los fundamentos de la versión 3 de ITIL.	Compra Directa	19/02/2018	21/02/2018	$ 750
Informe de viabilidad sobre la implementación de la metodología ITIL	El entregable se desarrolla con la asesoría del experto en seguridad informática.	Compra Directa	22/02/2018	23/02/2018	$ 75
Libro Manual de Revisión CISM, formulado por ISACA	Versión 2017 del libro, cuya temática aborda la gestión de un	Compra Directa	19/02/2018	18/05/2018	$ 140

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
	programa de seguridad de la información.				
Informe de viabilidad sobre la implementación del estándar ISO-27001	El entregable se desarrolla con la asesoría del experto en seguridad informática.	Compra Directa	22/02/2018	23/02/2018	$ 75
Análisis de viabilidad para la instalación de la herramienta “ACL”	El entregable se desarrolla con la asesoría del experto en seguridad informática e incluye el uso de una versión “Trial” de la herramienta.	Compra Directa	26/02/2018	02/03/2018	$ 100
Análisis de viabilidad para la instalación de la herramienta “IDEA”	El entregable se desarrolla con la asesoría del experto en seguridad informática e	Compra Directa	26/02/2018	02/03/2018	$ 100

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
	incluye el uso de una versión "Trial" de la herramienta.				
Análisis de viabilidad para la instalación de la herramienta "TOAD"	El entregable se desarrolla con la asesoría del experto en seguridad informática e incluye el uso de una versión "Trial" de la herramienta.	Compra Directa	26/02/2018	02/03/2018	$ 100
Estudio de herramientas para escaneo de vulnerabilidades en Servidores	El entregable se desarrolla con la asesoría del experto en seguridad informática e incluye el uso de una versión "Trial" de las herramientas evaluadas.	Compra Directa	05/03/2018	09/03/2018	$ 100
Estudio de	El entregable	Compra	05/03/2018	09/03/2018	$ 100

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
herramientas para escaneo de vulnerabilidades en Redes	se desarrolla con la asesoría del experto en seguridad informática e incluye el uso de una versión "Trial" de las herramientas evaluadas.	Directa			
Estudio de herramientas para escaneo de vulnerabilidades en Bases de Datos	El entregable se desarrolla con la asesoría del experto en seguridad informática e incluye el uso de una versión "Trial" de las herramientas evaluadas.	Compra Directa	05/03/2018	09/03/2018	$ 100
Elaboración de Políticas, Procedimientos y Manuales de Auditoría.	Los documentos se desarrollan con la asesoría del	Compra Directa	12/03/2018	04/04/2018	$ 125

Producto o Entregable	Descripción Técnica	Modalidad de Adquisición	Fechas Estimadas		Costo Aproximado
			Inicio	Fin	
	experto en seguridad informática.				
Elaboración de informe para la selección de una herramienta para la valoración de riesgos de TI.	El análisis incluye la valoración de las instrumentos “SEVRI”, “RISK IT”, “MARGERIT” y “AS/NZS”. Se desarrolla con la asesoría del experto en seguridad informática.	Compra Directa	09/04/2018	13/04/2018	$ 150
Plan de Revisión de los Recursos de TI, desde la perspectiva de seguridad.	El entregable es desarrollado por el asesor experto en seguridad informática	Compra Directa	18/04/2018	15/05/2018	$ 900

Fuente: (El Autor, 2018)

Se reafirma la importancia del rol desempeñado por el experto en seguridad informática reclutado para el proyecto y cuyo servicio profesional fue pactado por la suma de $ 2.000. Su asesoría se requiere para completar distintos entregables a lo largo del ciclo de vida del proyecto.

4.10 Plan de Gestión de los Interesados

La Gestión de los Interesados del Proyecto *"incluye los procesos necesarios para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto."* (PMI, 2013, Pág. No.390).

Existe mucha competitividad entre las organizaciones que brindan servicios de asesoría en el ámbito de las tecnologías de información, de la misma forma, no es extraño que la legislación nacional e internacional, marcos de referencia y estándares sufran modificaciones para hacer frente a las nuevas amenazas que aquejan a dicho sector; por consiguiente, ante dicho dinamismo es imperativo que el Director del Proyecto y su equipo de trabajo analice quienes son las personas y las entidades vinculadas directa o indirectamente al proyecto, acorde con sus expectativas e intereses:

Cuadro No. 46: Registro de los Interesados

Interesado	Descripción	Clasificación	Intereses	Expectativas
Socios de la Firma EEQA	Provee los recursos para la implementació	INTERNO	Ampliar el Portafolio de Servicios de la firma, a	Matricular a la Firma EEQA en el registro de auditores

Interesado	Descripción	Clasificación	Intereses	Expectativas
	n del proyecto y toma las decisiones en cuanto a inversiones y control del gasto.		través de la evaluación del Sistema de Gestión de la Seguridad de la Información.	elegibles de la SUGEF, específicamente en el campo de las tecnologías de información.
Director del Proyecto	Persona nombrada por los Socios de la Firma EEQA, lidera al equipo responsable de implementar el proyecto y alcanzar los objetivos establecidos.	INTERNO	Gestionar eficaz y eficientemente, las restricciones contrapuestas del proyecto, que incluyen el alcance, la calidad, el cronograma, el presupuesto, los recursos y los riesgos, entre otros.	Implementar exitosamente la propuesta de auditoría requerida por la Firma EEQA y que la misma posea potencial comercial.
Auditores Senior de la Firma EEQA	Grupo de profesionales que lideran la ejecución de las auditorías a los distintos clientes de la	INTERNO	Asimilar el plan de auditoría y ampliar sus conocimientos en materia de	Dirigir eficazmente la ejecución de los trabajos de auditoría.

Interesado	Descripción	Clasificación	Intereses	Expectativas
	firma.		tecnologías de información.	
Auditores Junior de la Firma EEQA	Proporcionan el apoyo requerido para completar la ejecución de las auditorías.	INTERNO	Asimilar el nuevo plan de auditoría y ampliar sus conocimientos en materia de tecnologías de información.	Planificar y ejecutar en conjunto con el Auditor Senior, las actividades a ser realizadas para el cumplimiento de los objetivos previstos con la auditoría.
Asesor en Seguridad Informática	Experto en la gestión de la información empresarial y de la integridad de la Infraestructura de TI, específicamente desde la perspectiva de seguridad.	EXTERNO	Con base en el marco normativo Costarricense y de las buenas prácticas de la gestión de las TI, desarrollar un plan para la revisión de un Sistema de Gestión de la	Implementar exitosamente el plan de auditoría requerida por la Firma EEQA, de conformidad con los lineamientos dados por la CGR y la SUGEF, entre otros entes

Interesado	Descripción	Clasificación	Intereses	Expectativas
			Información de TI.	reguladores.
Superintendencia General de Entidades Financieras (SUGEF)	Ente supervisor de la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional.	EXTERNO	Fiscalización en materia de legitimación de capitales y de las acciones que puedan servir para financiar actividades terroristas u organizaciones terroristas, establecidas en la Ley Nº 8204.	Que el plan de auditoría a desarrollar por la Firma EEQA, sirva de instrumento para la revisión sistema financiero nacional.
Contraloría General de la República (CGR)	Institución auxiliar de la Asamblea Legislativa, con absoluta independencia en la vigilancia y control de la hacienda pública.	EXTERNO	Cumplimiento de las Normas técnicas para la gestión y el control de las tecnologías de información, emitidas en 2007.	Que el plan de auditoría a desarrollar por la Firma EEQA, sirva de instrumento para la evaluación de las tecnologías de información, de conformidad con la Ley

Interesado	Descripción	Clasificación	Intereses	Expectativas
				General de Control Interno, Nº 8292.
Clientes de la Firma EEQA	Pertenecientes a diferentes sectores de la economía costarricense.	EXTERNO	Evaluar la razonabilidad de su SGSI (Sistema de Gestión de la Seguridad de la Información).	Cumplir las directrices giradas por la CGR y la SUGEF, entre otros entes reguladores.

Fuente: (El Autor, 2018)

Una vez identificados los involucrados del presente proyecto, se procede a clasificarlos según su nivel de poder e interés hacia el proyecto para poder establecer estrategias que posibiliten gestionarlos.

Para efectuar la ponderación de los niveles de “Poder” e “Interés”, se formularon una serie de consultas concisas y relevantes como criterio de evaluación, que permitieran determinar el comportamiento que muestra el interesado, las responsabilidades que asume como parte de la implementación del proyecto y la influencia que ejerce principalmente en la toma de decisiones, que afecten el rumbo que sigue el proyecto. Para una mejor interpretación de la respuesta obtenida, se estableció un instrumento de valoración cuantitativo de poca complejidad, que permitiera vincular la respuesta a una escala de calificación previamente definida y razonable:

Cuadro No. 47: Definición de los Valores de Poder

INTERESADO	PODER				TOTAL	
	¿Potencial para influir en el éxito del proyecto?	¿Su impacto en el proyecto no depende de la combinación de factores externos?	¿Su participación en el proyecto no puede ser asumida por otro involucrado?	¿Suministra recursos para el financiamiento y la dirección del proyecto?	Cuantitativo	Cualitativo
Socios de la Firma EEQA (A)	3	2	3	3	11	Alto
Director del Proyecto (B)	3	2	2	1	8	Alto
Auditores Senior de la Firma EEQA (C)	2	2	1	1	6	Bajo
Auditores Junior de la firma EEQA (D)	1	2	1	1	5	Bajo
Asesor en Seguridad Informática (E)	3	2	3	1	9	Alto
Superintendencia General de Entidades Financieras (F)	3	3	3	1	10	Alto
Contraloría General de la República (G)	3	3	3	1	10	Alto
Clientes de la Firma EEQA (H)	3	2	3	1	9	Alto

1 = Rara vez, 2 = Puede ocurrir, 3 = Probable

Escala de Valoración	
Rango	**Denominación**
7 a 12	**Alto**
1 a 6	**Bajo**

Fuente: (El Autor, 2018)

Cuadro No. 48: Definición de los Valores de Interés

INTERESADO	INTERÉS				TOTAL	
	¿Destina recursos para el seguimiento y el control del proyecto?	¿Considera prioritario la implementación del proyecto?	¿Constantemente se involucra en la toma de decisiones?	¿Existen distintos aspectos que le motivan a continuar u oponerse con el proyecto?	Cuantitativo	Cualitativo
Socios de la firma EEQA (A)	3	3	3	3	12	Alto
Director del Proyecto (B)	2	3	3	3	11	Alto
Auditores Senior de la Firma EEQA (C)	1	3	2	2	8	Alto
Auditores Junior de la firma EEQA (D)	1	3	1	1	6	Bajo
Asesor en Seguridad Informática (E)	1	2	2	1	6	Bajo
Superintendencia General de Entidades Financieras (F)	1	2	1	2	6	Bajo
Contraloría General de la República (G)	1	2	1	2	6	Bajo
Clientes de la Firma EEQA (H)	1	2	1	2	6	Bajo

1 = Rara vez, 2 = Puede ocurrir, 3 = Probable

Escala de Valoración	
Rango	**Denominación**
7 a 12	**Alto**
1 a 6	**Bajo**

Fuente: (El Autor, 2018)

Los resultados obtenidos se ilustran a través de la matriz denominada “Poder – Influencia”, la cual muestra a los interesados acorde a su nivel de autoridad y preocupación con respecto al proyecto:

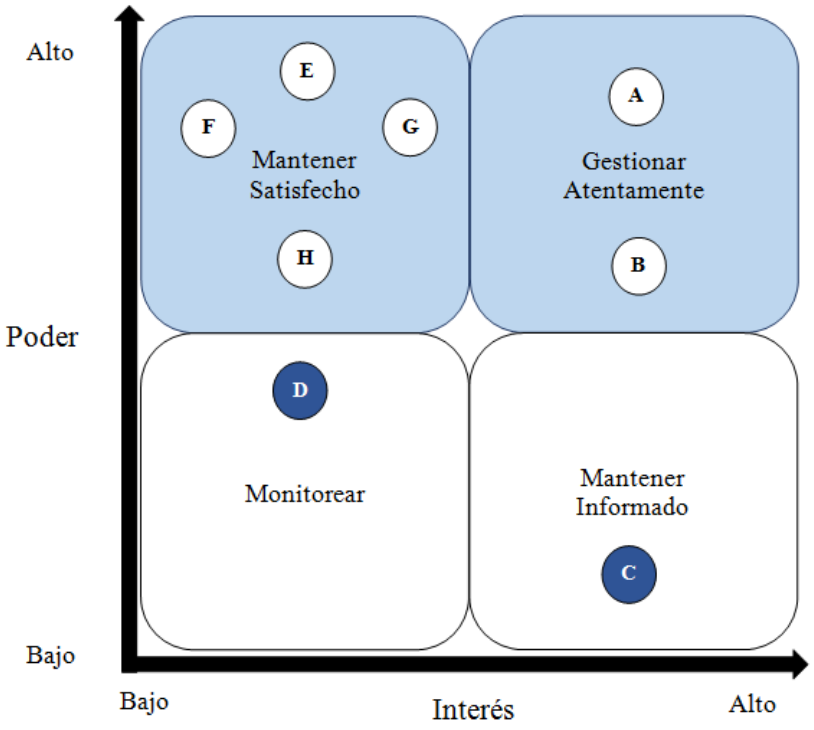


Figura No. 11. Matriz Poder - Interés

Fuente: (El Autor, 2018)

Seguidamente, se procede a desarrollar las estrategias de gestión para lograr la participación eficaz de los interesados a lo largo del ciclo de vida del proyecto y mitigar los impactos negativos, con base en los resultados de la matriz antes desarrollada:

- **Gestionar Atentamente:** A este nivel, la comunicación debe transitar fluidamente por cuanto se toman decisiones clave para el éxito del proyecto; asimismo, se requiere que la documentación del proyecto se encuentre actualizada y disponible para ser consultada. Debe existir claridad en todos los objetivos del proyecto, así como en la gestión de todas las restricciones contrapuestas. Para ello, se debe coordinar reuniones de conformidad con la periodicidad previamente establecida.

- **Mantener Informados:** No se ostenta un amplio poder para la toma de decisiones que modifiquen el curso del proyecto; sin embargo, el conocimiento técnico que acumula los ubicados en este cuadrante justifica el obtener sus criterios conforme el proyecto avanza, lo que demanda la retroalimentación oportuna entre las partes involucradas.

- **Mantener Satisfecho:** Agrupa a personas y entidades con un alto poder para influir en el éxito o fracaso del proyecto, como es el caso de los clientes de la firma y de los entes reguladores; motivo por el cual debe destinarse esfuerzos de parte del equipo del proyecto en conocer sus expectativas, necesidades y observaciones; lo anterior con la finalidad de identificar a tiempo desviaciones que repercutan negativamente en la implementación del proyecto. Lo anterior implica el sondear la configuración de la infraestructura tecnológica de los clientes de la firma y determinar si existe congruencia con la propuesta de auditoría que se pretende desarrollar.

- **Monitorear:** Se categorizan con niveles bajo de interés y poder, por lo que se requiere trabajar aspectos motivacionales que generen pertenencia al proyecto. Por ejemplo, incentivar el involucramiento en los procesos de toma de decisiones acorde con la sensibilidad y criticidad de los puntos que deban ser evaluados.

5. CONCLUSIONES

A continuación, se presentan las siguientes conclusiones como resultado de la formulación del Plan de Gestión del Proyecto:

1. El proyecto denominado “Propuesta de un Plan de Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información”, pretende subsanar la necesidad de la Firma consultora EEQA, de incorporar dicha revisión como parte de su portafolio de servicios profesionales; para implementar un proyecto de tal complejidad técnica, es fundamental el seguimiento de las buenas prácticas consignadas en la quinta edición de la guía PMBOK, lo que repercute positivamente en la probabilidad de éxito para el proyecto. Lo anterior implica el desarrollo de los planes de gestión de la integración, gestión del alcance, gestión del tiempo, gestión de los costos, gestión de la calidad, gestión de los recursos humanos, gestión de las comunicaciones, gestión de los riesgos, gestión de las adquisiciones y de la gestión de los interesados, todos ellos incorporados como objetivos específicos en el Acta del Proyecto.

2. Es trascendental que la Firma EEQA logre matricularse en el registro de auditores elegibles de la SUGEF. De esta forma, existirá el aval pertinente para participar como Auditoría Externa y evaluar los sistemas de tecnologías de información. De lo contrario, el retorno de la inversión efectuada por los socios de la firma no sería el proyectado, al no convertirse en un servicio profesional con potencial para ser comercializado. Las lecciones aprendidas al desarrollar dicho proyecto, pasarán a formar parte de los activos empresariales de la Firma EEQA.

3. De conformidad con el Plan de Gestión del Alcance, se estructuró una propuesta para auditar un Sistema de Gestión de Seguridad de la Información, que especificaba claramente cuáles son los componentes a

evaluar; asimismo, para definir el trabajo requerido para completar el proyecto exitosamente y descartar otros productos de auditoría sobre los cuales la Firma EEQA no poseía los recursos necesarios para poder implementar.

4. La Firma EEQA promueve la investigación del Software Libre como plataforma para la tecnificación de la función de las organizaciones, debido a sus condiciones de libertad de uso, distribución y mejora continua. Al respecto, el cronograma del proyecto se elaboró mediante la aplicación “OpenProj” basada en Java. De esta forma y de conformidad con el Plan de Gestión del Cronograma, se establecieron las actividades que conforman el proyecto y su secuencia, a la vez que se definieron los recursos necesarios para completarlas. Se estimó la duración aproximada del proyecto en 74 días, iniciando el 19 de febrero de 2018 y como fecha tentativa de finalización el 06 de junio de 2018.

5. El presupuesto es una de las principales restricciones contrapuestas que debe ser gestionado eficazmente por el equipo del proyecto. Estimar correctamente los costos a través de la asignación de los valores que cubren a los entregables, así como el establecimiento de reservas de contingencia y de gestión, proporcionan confiabilidad al patrocinador (en este caso los socios de la Firma EEQA), que verdaderamente existe factibilidad de implementar el proyecto.

6. El Plan de Gestión de la Calidad permitió definir los requisitos de calidad del proyecto, las métricas de calidad del proyecto y las actividades de prevención y control de la calidad para los entregables; en esencia, la Firma EEQA maneja altos estándares por cuanto sus asesorías únicamente encontrarán mercado si satisfacen los requerimientos establecidos por sus clientes, principalmente en el ámbito financiero, segmento ampliamente sensible a ataques informáticos mediante la explotación de vulnerabilidades y brechas de seguridad.

7. A partir del Plan de Gestión de los Recursos Humanos, se definió el organigrama organizacional del proyecto, así como las funciones a desarrollar las cuales fueron asumidas principalmente por el personal de la Firma EEQA; no obstante, cabe destacar la incorporación del Asesor en Seguridad Informática, quien aportó conocimiento esencial para completar actividades de importancia muy significativa para el proyecto. Todo lo anterior se plasmó en una matriz de roles y responsabilidades.

8. Al incorporar un Plan de Gestión de los Interesados, se identificaron oportunamente las personas con el conocimiento, experiencia e interés en desarrollar el presente proyecto. De esta forma, la asignación de responsabilidades se precisó acorde a tres ejes primordiales: Auditoría, Soporte Tecnológico y Soporte Administrativo. Particularmente, se logra generar un manejo de las expectativas de los principales involucrados, descartándose síntomas de resistencia al cambio y propiciando un contexto participativo y colaborativo entre el personal de la Firma EEQA, principalmente en lo referente a la toma decisiones.

9. Aprovechando la experiencia acumulada por el equipo de auditores de la Firma EEQA, se desarrolló un análisis profundo de los riesgos que rodean la implementación del proyecto a través de su ciclo de vida, utilizando para ello criterios de índole cualitativo y cuantitativo. De la misma forma, una vez identificados y priorizados dichos riesgos, se determinaron los controles correspondientes que permitieran que el nivel de riesgo inherente fuera razonable, con base en acciones oportunas de orden preventivo y correctivo.

10. Con base en el análisis de Hacer-Comprar propio del Plan de Gestión de las Adquisiciones, se determinó que muchos de los principales de entregables del proyecto se podían generar a partir de recursos propios. En

cuanto los elementos que deben ser adquiridos, se establecieron las reglas y condiciones para materializar dichas compras y se definió el tipo de contrato requerido para salvaguardar los intereses de las partes involucradas, todo lo cual proporciona un marco de control a lo interno del proyecto.

11. Se reconoce que la comunicación es fundamental para el éxito del proyecto, en tal sentido la experiencia obtenida por la Firma EEQA en solicitar y gestionar la documentación de sus clientes y en comunicar efectivamente los hallazgos de sus auditorías, se orientó al servicio del proyecto, lo cual se plasma en el Plan de la Gestión de las Comunicaciones, posibilitando el controlar la información del proyecto en todos sus extremos.

6. RECOMENDACIONES

Una vez finalizado el proyecto, se generan las siguientes recomendaciones:

1. Acorde con su naturaleza de negocios, la Firma EEQA promueve entre sus clientes la aplicación de estándares y buenas prácticas, destacándose principalmente aquellas de orden financiero y de auditoría lo cual es congruente con su giro de negocios; no obstante, se observó que lo concerniente al uso de las buenas prácticas para la administración de proyectos consignadas en la quinta edición de la guía PMBOK, es apenas una metodología incipiente en la consultora. De ahí que es necesario reforzar dicha temática en toda la organización por cuanto administrar proyectos se ha convertido en un requerimiento global, independientemente del sector al que pertenezca una organización y PMBOK proporciona pautas para la dirección de proyectos, describe el ciclo de vida de la dirección de proyectos y los procesos relacionados

2. Al ser el campo de las consultorías una de las principales actividades en el contexto de negocios para la Firma EEQA, resulta oportuno y razonable optar por la creación de una Oficina de Proyectos (PMO), con la intención de brindar soporte profesional tanto al cliente interno como al externo. OPM3 es un modelo para la formulación de un estudio de madurez de la organización, para determinar el manejo sistemático de los proyectos, programas y portafolios, al proveer una forma de avanzar hacia los objetivos estratégicos de la organización, fundamentándose en la aplicación de los principios y las prácticas de la dirección de proyectos.

3. La revisión y actualización periódica de los procedimientos de la Firma EEQA, se constituye en una tarea fundamental para el fortalecimiento del marco normativo instaurado en la empresa, lo cual a su vez posibilita el

promover el debido cumplimiento de dicho marco y con ello gestionar eficaz y eficientemente los recursos de los cuales dispone dicha consultora.

Por consiguiente, debe elaborarse un plan indicando los documentos relacionados con la ejecución de auditorías y con la gestión de proyectos que deben ser objeto de actualización; asimismo, es importante que se consigne a nivel de procedimiento, cuáles son los documentos que obligatoriamente deberán elaborarse, independientemente de los requerimientos a nivel procedimental que establezcan tanto el cliente como los proveedores de la Firma EEQA.

4. En el ámbito de las tecnologías de información, las certificaciones juegan un papel clave para posicionar a un proveedor de servicios como un agente de confianza; en ese sentido, es fundamental que la Firma EEQA a través de un Plan de Gestión del Recurso Humano, proporcione el conocimiento necesario a su personal, para que el plan de auditoría a desarrollar se ejecute de conformidad a las expectativas de sus clientes, máxime cuando se pretende incorporar herramientas tecnológicas que implican mayor complejidad y profundidad al trabajo de auditoría.

5. Una vez que se ha confirmado el conocimiento y la experiencia del Asesor en Seguridad Informática, cuyos aportes fueron fundamentales para el establecer el contenido temático del plan de auditoría a desarrollar y que se evidencia a través del cuadro No.22 del presente documento, la Firma EEQA debe trazar una línea del perfil de profesional que se requiere para desarrollar trabajos de auditoría y consultoría en el campo de las tecnologías de información. En la actualidad la firma carece de personal con dichas características, por lo que incorporar profesionales con estas competencias le permitirán adquirir mayor conocimiento y obtener credibilidad entre sus clientes.

6. El costo vinculado con el licenciamiento del hardware y software, es una de las principales limitantes que deben enfrentar las organizaciones, por lo que frecuentemente se materializa el riesgo de obsolescencia tecnológica. Ante el deseo de la Firma EEQA de incorporar herramientas tecnológicas como parte de su propuesta de auditoría, es indispensable el análisis de dichos costos de licenciamiento independientemente de la modalidad de la licencia (monousuario, multiusuario), máxime cuando el alcance considera herramientas para el monitoreo y análisis de vulnerabilidades en servidores, equipo de telecomunicaciones y bases de datos, entre otros recursos.

7. El alcance del proyecto se encuentra bien delimitado; es decir, desarrollar un Plan de Dirección para auditar un Sistema de Gestión de Seguridad de la Información. Una vez evaluados los recursos con los que cuenta la Firma EEQA, no se recomienda a corto plazo el ampliar su portafolio de negocios con la prestación de servicios administrados adicionales, como es el caso de aprovisionamiento de soluciones especializadas de TI, desarrollo de software a la medida o el diseño y equipamiento de Centro de Datos, entre otros.

   La Firma EEQA tiene aún mucho camino por recorrer en lo referente la gestión de tecnologías de información y la curva de aprendizaje es amplia. Ofrecer este tipo de servicios va acarrear para EEQA el desempeñar un papel de “integrador” de servicios tecnológicos, requiriendo para ello del aporte de distintos intermediarios que le posibiliten consolidar su portafolio de servicios, lo que representa un riesgo de dependencia tecnológica sobre proveedores, tema continuamente advertido por la Contraloría General de la República.

8. Se recomienda a la Firma EEQA el optimizar el uso de herramientas para entablar sesiones de trabajo remotas, lo cual en ocasiones presentó inconvenientes en las reuniones del equipo de trabajo del proyecto. El

personal de la firma normalmente visita a sus clientes en sus oficinas; no obstante, el uso de herramientas para la comunicación de personas geográficamente dispersas rige al actual mercado de negocios globalizado, principalmente en las organizaciones fuertemente influenciadas por las tecnologías de información, segmento de negocios en el cual planea incursionar la Firma EEQA.

9. Si al finalizar la etapa de formulación de la propuesta, los Socios de la Firma acuerdan continuar con su implementación, es prudente aplicar herramientas tales como el análisis del “Valor Ganado”, ya que permiten establecer la variación del cronograma (SV) en cada una de las actividades; asimismo, el índice de desempeño del cronograma (SPI) va a determinar si el proyecto corre el riesgo de sufrir algún retraso o en su defecto, la posibilidad de concluir antes de lo planeado en relación con la línea base original del cronograma.

7. BIBLIOGRAFIA

Asamblea Legislativa. (2011). Ley No.8968 de protección de la persona frente al tratamiento de sus datos personales: Costa Rica: Diario La Gaceta. Su ámbito de aplicación corresponde a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados.

Asamblea Legislativa. (2012). Ley No.9048, reforma de la Sección VIII, Delitos Informáticos y Conexos, del Titulo VII del Código Penal: Costa Rica: Diario La Gaceta. Especifica las sanciones para quienes cometan delitos relacionados con la violación de correspondencia o comunicaciones, estafa informática, daño informático, espionaje, suplantación de identidad, instalación o propagación de programas maliciosos, suplantación de páginas electrónicas y difusión de información falsa, entre otras situaciones estrechamente relacionadas con las tecnologías de información.

Bernal, César A. (2010). Normas Metodología de la Investigación: Colombia: Pearson. Contribuye con el diseño de una estrategia para la recolección y análisis de los datos.

Consejo Nacional de Supervisión del Sistema Financiero. (2009). Acuerdo SUGEF 14-09, Reglamento sobre la gestión de la tecnología de información: Costa Rica: Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF). Define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas por SUGEF.

Contraloría General de la República. (2006). Manual de normas generales de auditoría para el sector público: Costa Rica: Contraloría General de la República (CGR). Dicha normativa establece los lineamientos para la función de la auditoría.

Contraloría General de la República. (2007). Normas técnicas para la gestión y el control de las Tecnologías de Información: Costa Rica: Contraloría General de la República (CGR). Dicha normativa establece los criterios básicos de control para la gestión de las tecnologías de información.

Esterkin, José. (2010). Qué son los entregables del proyecto. Recuperado de: https://iaap.wordpress.com/2010/09/16/%C2%BFque-son-los-entregablesdel-proyecto/. Establece criterios básicos circunscritos a la gestión de proyectos.

Eyssautier de la Mora, Maurice. (2002). Metodología de la investigación. Desarrollo de la inteligencia. México: Thomson. Aporta teoría para establecer las bases del proceso de investigación del presente documento.

Hernández Sampieri, Roberto. (1999). Metodología de la Investigación. México: Mc Graw Hill. Consigna teoría para desarrollar el proceso de investigación del trabajo.

International Organization for Standardization. (2013). ISO/IEC 27001. Suiza: Information technology - Security techniques - Information security management systems. Establece buenas prácticas en relación con la seguridad de información.

ISACA. (2012). COBIT 5: Illinois: Information Systems Audit and Control Association. Este marco de referencia consigna buenas prácticas en relación con la gestión del gobierno de TI, el cual es un elemento primordial en el alcance de una auditoría.

ISACA. (2016). Manual de Preparación para el examen CISM: Illinois: Information Systems Audit and Control Association. La incorporación del documento se justifica en el programa de seguridad de la información que proporciona, el cual fue desarrollado por el esfuerzo voluntario de miembros de la comunidad ISACA.

ISACA. (2016). Manual de Preparación para el examen CRISC: Illinois: Information Systems Audit and Control Association. Proporciona una guía de referencia para la gestión del riesgo de TI, lo que representa uno de los principales ejes temáticos abordados en el PFG.

ITpreneurs. (2012). Manual de Alumno: Curso ITIL Foundation Versión 3.2.1: Nederland: ITpreneurs. Resume los conceptos básicos sobre la gestión de los servicios de TI, acorde con la metodología ITIL.

Lledó, P. (2013). Director de Proyectos: Cómo aprobar el examen PMP sin morir en el intento. Victoria: Pablo Lledó. PMP corresponde a la certificación profesional más reconocida para la administración de proyectos; asimismo, este documento aporta ejercicios concisos que posibilitan una efectiva asimilación de los conceptos teóricos.

López Careño, Rosana. (2017). Fuentes de información. Guía básica y nueva clasificación. España: UOC Editorial. Suministra importante conocimiento en relación con la identificación de las fuentes de información, los distintos tipos existentes y su finalidad.

Project Management Institute Inc. (2013). Quinta edición de la guía de los fundamentos para la dirección de proyectos (Guía PMBOK). Pennsylvania: Project Management Institute. PMBOK proporciona un lenguaje común en lo referente a la gestión de proyectos, por lo que su inclusión en el presente trabajo es fundamental.

Rossi, José. (2014). Inversión Extranjera Directa en Costa Rica: Evolución y Retos. Costa Rica: Coalición Costarricense de Iniciativas de Desarrollo (CINDE). Detalla la inversión extranjera efectuada en Costa Rica, destacándose el sector de la alta tecnología.

SUGEF. (2017). Reglamento General de Gestión de la Tecnología de Información (Acuerdo SUGEF 14-17). Costa Rica: Superintendencia General de

Entidades Financieras (SUGEF). Establece los criterios para gestionar el riesgo de las tecnologías de información, así como los procesos de gobierno de TI.

ANEXOS

Anexo 1: ACTA DEL PFG

<table>
<tr><th colspan="2">ACTA DEL PROYECTO</th></tr>
<tr><th>Fecha</th><th>Nombre de Proyecto</th></tr>
<tr><td>06/11/2017</td><td>Propuesta de un Plan de Dirección de un Proyecto para Auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para la Firma de Consultoría EEQA.</td></tr>
<tr><th>Areas de conocimiento / procesos:</th><th>Area de aplicación (Sector / Actividad):</th></tr>
<tr><td>Grupos de Procesos: Iniciación, planificación.

Areas de Conocimiento: Integración, alcance, plazo, costo, calidad, riesgos, comunicaciones, recursos humanos, adquisiciones e interesados.</td><td>Consultoría.
Auditoría.
Tecnologías de Información.</td></tr>
<tr><th>Fecha de inicio del proyecto</th><th>Fecha tentativa de finalización del proyecto</th></tr>
<tr><td>06/11/2017</td><td>15/07/2018</td></tr>
<tr><th colspan="2">Objetivos del proyecto (general y específicos)</th></tr>
<tr><td colspan="2">Objetivo general

Crear una propuesta de un plan de dirección de un proyecto para auditar un Sistema de Gestión de Seguridad de la Información (SGSI), para que la firma consultora EEQA pueda implementarlo como parte de su cartera de servicios profesionales.

Objetivos específicos

1. Desarrollar un plan de gestión del alcance para identificar las actividades necesarias para la ejecución del proyecto, considerando para ello los requerimientos consignados en los marcos normativos y de buenas prácticas, tanto en el ámbito nacional como internacional.
2. Elaborar un plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma.
3. Desarrollar un plan de gestión de costos para determinar el presupuesto requerido para auditar un Sistema de Gestión de Seguridad de la Información.
4. Preparar un plan de gestión de la calidad para identificar el grado y el nivel de exigencia que demanda un plan de auditoría que debe propiciar oportunidades de negocio.
5. Realizar un plan de gestión de los recursos humanos para identificar los aportes y las limitaciones del personal que forma parte de la firma EEQA, que participará en el proyecto.
6. Generar un plan de gestión de comunicación para identificar y optimizar el uso de los canales de contacto y los documentos del proyecto.
7. Crear un plan de gestión de riesgos para administrarlos de forma oportuna; asimismo, para definir las herramientas que permitan gestionar razonablemente los riesgos vinculados con la función de TI.
8. Desarrollar un plan de gestión de adquisiciones para identificar los flujos de los insumos requeridos por el proyecto y los niveles de responsabilidad de las partes involucradas.
9. Elaborar un plan de gestión de los interesados para determinar las necesidades acorde con los roles establecidos.</td></tr>
<tr><th colspan="2">Justificación o propósito del proyecto (Aporte y resultados esperados)</th></tr>
</table>

La información es un recurso invaluable para que las organizaciones puedan tomar decisiones, continuar operando y alcanzar sus objetivos estratégicos; asimismo, otro aspecto destacable es el auge de la tecnología como medio para su administración.

Al respecto, es lógico determinar el incremento de los riesgos y amenazas contra la integridad, disponibilidad y confidencialidad de la información, por lo que la implementación de un Sistema de Gestión de Seguridad de la Información, es una buena práctica para adoptar controles de orden preventivo y correctivo que permitan dar respuesta al robo de datos, brechas de seguridad y ataques cibernéticos, entre otros eventos.

La consultora EEQA es una firma radicada en Costa Rica, que actualmente se especializa en la prestación de servicios contables, lo cual incluye auditorías para determinar la razonabilidad de los estados financieros. EEQA es considerada una firma menor, cabe indicar que en Costa Rica tienen presencia las 4 consultoras más grandes del mundo: PWC, Ernst & Young, KPMG y Deloitte. A pesar de ello, la firma ha logrado consolidar una importante cartera de clientes; sin embargo, algunas oportunidades de negocios han sido desaprovechadas debido a que EEQA no ostenta como parte de su catálogo de servicios, asesorías sobre la gestión de las tecnologías de información, en su nómina tampoco figura algún profesional experto en dicha temática.

Por consiguiente, la firma desea desarrollar su propia propuesta que le permita asesorar a sus clientes en relación con el estado actual del "Sistema de Gestión de Seguridad de la Información", de igual forma, generar nuevas oportunidades de negocio e incrementar los niveles de ingreso y rentabilidad. Es relevante indicar que existen diferentes marcos metodológicos y buenas prácticas que servirán de insumo al proyecto para formular una propuesta de auditoría cuya implementación sea viable comercializar.

Descripción del producto o servicio que generará el proyecto – Entregables finales del proyecto

El producto final del proyecto es un documento con una propuesta de un plan de dirección de un proyecto para auditar un "Sistema de Gestión de Seguridad de la Información", que considere el gobierno de seguridad de la información, la gestión de riesgos de la información y su cumplimiento, el desarrollo y la gestión del programa de seguridad de la información y la gestión de incidentes.

Los entregables que lo conforman son los planes de gestión de las 10 áreas de conocimiento consignadas en la quinta edición de la Guía de Fundamentos PMBOK, para lo cual se formularan las plantillas respectivas.

Finalmente, se establecerá el perfil y competencias del recurso humano que se encargará de desarrollar las revisiones de auditoría de conformidad con el plan a implementar.

Supuestos

El personal de la firma consultora suministrará información veraz en relación con las necesidades identificadas; asimismo, no existe resistencia en lo concerniente a incursionar en el asesoramiento de tecnologías de información.

El plazo establecido para efectuar el plan de proyecto es razonable y permitirá alcanzar los resultados planificados.

La calidad de la información existente es adecuada y pertinente para poder realizar los planes gestión del proyecto e identificar oportunidades de mejora.

Restricciones

El plazo para finalizar el proyecto termina el 15 de julio de 2018.

La firma consultora EEQA carece de experiencia en relación con la ejecución de auditorías en el ámbito de las tecnologías de información.

Existe en Costa Rica un Marco Normativo de acatamiento obligatorio, que incluye las normas técnicas para la gestión y el control de las tecnologías de información y el acuerdo de la SUGEF 14-17 correspondiente al reglamento de gestión de las tecnologías de información, entre otros, los cuales son documentos que deben ser considerados al formular un plan de auditoría aplicable en Costa Rica.

Identificación riesgos

5. Si la firma consultora EEQA no proporciona la información necesaria para el proyecto, podría afectar su alcance, el presupuesto y la calidad final del documento.
6. Las tecnologías de información se caracterizan por su dinamismo, por lo que nuevos requerimientos principalmente desde la perspectiva de seguridad, pueden originar modificaciones a la propuesta de auditoría.
7. El desconocimiento e inexperiencia en el tema tecnológico por parte de algunos miembros de la firma EEQA, principalmente de quienes toman decisiones, podría generar desinterés en la implementación del proyecto, máxime si el mismo adquiere mayor complejidad conforme su desarrollo avanza.
8. De incrementarse el costo de la implementación de la propuesta, podría afectarse su implementación como parte de la cartera de servicios de la firma de consultora EEQA.

Presupuesto

Descripción	Monto
Curso de Fundamentos ITIL para la gestión de servicios de TI	$ 750
Libro Manual de Revisión CISM, formulado por ISACA	$ 140
Servicios de Telecomunicaciones (Internet)	$ 60
Imprevistos	$ 100
Total	**US$ 1,050**

Principales hitos y fechas

Nombre hito	Fecha inicio	Fecha final
Plan de gestión del alcance del proyecto	05 de marzo de 2018	11 de marzo de 2018
Plan de gestión del cronograma para planificar, ejecutar y controlar las actividades del cronograma	12 de marzo de 2018	18 de marzo de 2018
Plan de gestión de costos para determinar el presupuesto requerido por el proyecto	19 de marzo de 2018	25 de marzo de 2018
Plan de gestión de la calidad del proyecto	26 de marzo de 2018	01 de abril de 2018
Plan de gestión de los recursos humanos del proyecto	02 de abril de 2018	08 de abril de 2018
Plan de gestión de comunicación del proyecto	09 de abril de 2018	15 de abril de 2018
Plan de gestión de riesgos del proyecto	16 de abril de 2018	25 de abril de 2018
Plan de gestión de adquisiciones requeridos por el proyecto	26 de abril de 2018	06 de mayo de 2018
Plan de gestión de los interesados del proyecto	07 de mayo de 2018	13 de mayo de 2018
Propuesta de un Plan de Dirección de un Proyecto para Auditar un “Sistema de Gestión de Seguridad de la Información”	14 de mayo de 2018	24 de mayo de 2018

Información histórica relevante

La Firma de Consultoría EEQA nace como parte de la iniciativa de un grupo de profesionales en contaduría pública y auditoría,

con amplia experiencia en Costa Rica. Entre sus servicios profesionales se encuentran las auditorías financieras, servicios contables, certificaciones de ingreso, elaboración de planillas y control interno.

Sus oficinas centrales se localizan en la provincia de San José y figuran como sus principales clientes empresas del sector automovilístico y de logística de servicios de transporte. Recientemente, EEQA implementó los servicios de asesoría legal y su siguiente paso como parte de su estrategia de crecimiento, consiste en la incursión en el campo de las Tecnologías de Información.

El Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), mediante artículo 6, del acta de la sesión 773-2009 del 20 de febrero del 2009 aprobó el Acuerdo SUGEF 14-09 "Reglamento sobre la gestión de la tecnología de información", que define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras (SUGEF). Asesorar a entidades financieras que deben cumplir con la norma supra citada, motivó a la firma EEQA a desarrollar su propia propuesta de auditoría para aplicarla comercialmente.

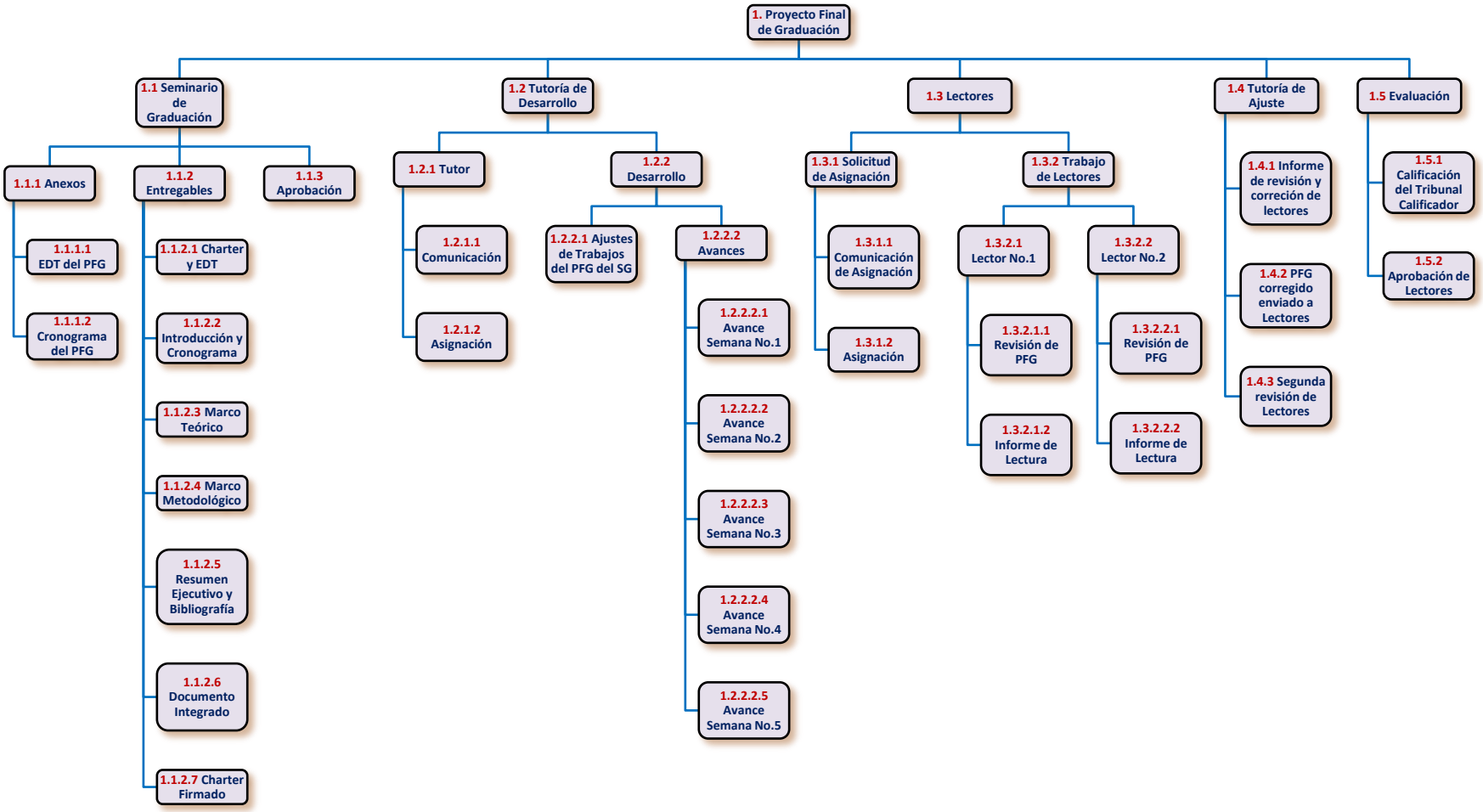
Identificación de grupos de interés (involucrados)

Involucrados directo(s):
Socios de la firma EEQA.
Auditores Senior de la firma EEQA.
Auditores Junior de la firma EEQA.
Clientes de la firma EEQA.

Involucrados indirecto(s):
Superintendencia General de Entidades Financieras (SUGEF).
Contraloría General de la República (CGR).

Director de proyecto: **Maikol Fernando Hernández Segura**	**Firma:** 
Autorización de: **Yorlenny Hidalgo**	**Firma:**

Anexo 2: EDT


1. Proyecto Final de Graduación
1.1 Seminario de Graduación
1.1.1 Anexos
1.1.1.1 EDT del PFG
1.1.1.2 Cronograma del PFG
1.1.2 Entregables
1.1.2.1 Charter y EDT
1.1.2.2 Introducción y Cronograma
1.1.2.3 Marco Teórico
1.1.2.4 Marco Metodológico
1.1.2.5 Resumen Ejecutivo y Bibliografía
1.1.2.6 Documento Integrado
1.1.2.7 Charter Firmado
1.1.3 Aprobación
1.2 Tutoría de Desarrollo
1.2.1 Tutor
1.2.1.1 Comunicación
1.2.1.2 Asignación
1.2.2 Desarrollo
1.2.2.1 Ajustes de Trabajos del PFG del SG
1.2.2.2 Avances
1.2.2.2.1 Avance Semana No.1
1.2.2.2.2 Avance Semana No.2
1.2.2.2.3 Avance Semana No.3
1.2.2.2.4 Avance Semana No.4
1.2.2.2.5 Avance Semana No.5
1.3 Lectores
1.3.1 Solicitud de Asignación
1.3.1.1 Comunicación de Asignación
1.3.1.2 Asignación
1.3.2 Trabajo de Lectores
1.3.2.1 Lector No.1
1.3.2.1.1 Revisión de PFG
1.3.2.1.2 Informe de Lectura
1.3.2.2 Lector No.2
1.3.2.2.1 Revisión de PFG
1.3.2.2.2 Informe de Lectura
1.4 Tutoría de Ajuste
1.4.1 Informe de revisión y correción de lectores
1.4.2 PFG corregido enviado a Lectores
1.4.3 Segunda revisión de Lectores
1.5 Evaluación
1.5.1 Calificación del Tribunal Calificador
1.5.2 Aprobación de Lectores

Anexo 3: CRONOGRAMA

	Nombre	Duración	Inicio	Terminado	Predecesores
1	**Proyecto Final de Graduación**	230 days?	**06/11/17 08:00 AM**	**23/06/18 05:00 PM**	
2	**Seminario de Graduación**	35 days?	**06/11/17 08:00 AM**	**10/12/17 05:00 PM**	
3	**Anexos**	1 day?	**20/11/17 08:00 AM**	**20/11/17 05:00 PM**	
4	EDT del PFG	1 day?	20/11/17 08:00 AM	20/11/17 05:00 PM	
5	Cronograma del PFG	1 day?	20/11/17 08:00 AM	20/11/17 05:00 PM	
6	**Entregables**	35 days?	**06/11/17 08:00 AM**	**10/12/17 05:00 PM**	
7	Charter y EDT	7 days?	06/11/17 08:00 AM	12/11/17 05:00 PM	
8	Introducción y Cronograma	7 days?	13/11/17 08:00 AM	19/11/17 05:00 PM	7
9	Marco Teórico	7 days?	20/11/17 08:00 AM	26/11/17 05:00 PM	8
10	Marco Metodológico	7 days?	27/11/17 08:00 AM	03/12/17 05:00 PM	9
11	Resumen Ejecutivo y Bibliografía	7 days?	04/12/17 08:00 AM	10/12/17 05:00 PM	10
12	Documento Integrado	7 days?	04/12/17 08:00 AM	10/12/17 05:00 PM	10
13	Charter Firmado	7 days?	04/12/17 08:00 AM	10/12/17 05:00 PM	10
14	Aprobación	7 days?	04/12/17 08:00 AM	10/12/17 05:00 PM	10
15	**Tutoría de Desarrollo**	88 days?	**26/02/18 08:00 AM**	**24/05/18 05:00 PM**	
16	HITO I - ENTREGABLES	0 days?	26/02/18 08:00 AM	26/02/18 08:00 AM	
17	**Tutor**	2 days?	**26/02/18 08:00 AM**	**27/02/18 05:00 PM**	
18	Comunicación	1 day?	26/02/18 08:00 AM	26/02/18 05:00 PM	3;6
19	Asignación	1 day?	27/02/18 08:00 AM	27/02/18 05:00 PM	18
20	**Desarrollo**	88 days?	**26/02/18 08:00 AM**	**24/05/18 05:00 PM**	
21	Ajustes de Trabajos del PFG del SG	5 days?	28/02/18 08:00 AM	04/03/18 05:00 PM	3;6
22	**Avances**	88 days?	**26/02/18 08:00 AM**	**24/05/18 05:00 PM**	
23	Avance Semana No.1	14 days?	05/03/18 08:00 AM	18/03/18 05:00 PM	21
24	Avance Semana No.2	14 days?	19/03/18 08:00 AM	01/04/18 05:00 PM	23
25	Avance Semana No.3	14 days?	02/04/18 08:00 AM	15/04/18 05:00 PM	24
26	Avance Semana No.4	21 days?	16/04/18 08:00 AM	06/05/18 05:00 PM	25
27	Avance Semana No.5	18 days?	07/05/18 08:00 AM	24/05/18 05:00 PM	26
28	HITO II - AVANCES	0 days	26/02/18 08:00 AM	26/02/18 08:00 AM	
29	**Lectores**	14 days?	**25/05/18 08:00 AM**	**07/06/18 05:00 PM**	
30	**Solicitud de Asignación**	1 day?	**25/05/18 08:00 AM**	**25/05/18 05:00 PM**	
31	Comunicación de Asignación	1 day?	25/05/18 08:00 AM	25/05/18 05:00 PM	20
32	Asignación	1 day?	25/05/18 08:00 AM	25/05/18 05:00 PM	20
33	**Trabajo de Lectores**	11 days?	**28/05/18 08:00 AM**	**07/06/18 05:00 PM**	
34	**Lector No.1**	11 days?	**28/05/18 08:00 AM**	**07/06/18 05:00 PM**	
35	Revisión de PFG	10 days?	28/05/18 08:00 AM	06/06/18 05:00 PM	20;30
36	Informe de Lectura	1 day?	07/06/18 08:00 AM	07/06/18 05:00 PM	20;30
37	**Lector No.2**	11 days?	**28/05/18 08:00 AM**	**07/06/18 05:00 PM**	
38	Revisión de PFG	10 days?	28/05/18 08:00 AM	06/06/18 05:00 PM	20;30
39	Informe de Lectura	1 day?	07/06/18 08:00 AM	07/06/18 05:00 PM	20;30
40	**Tutoría de Ajuste**	213 days?	**20/11/17 08:00 AM**	**20/06/18 05:00 PM**	
41	Informe de Revisión y Corrección de Lectores	7 days?	08/06/18 08:00 AM	14/06/18 05:00 PM	34;37
42	PFG Corregido Enviado a Lectores	1 day?	15/06/18 08:00 AM	15/06/18 05:00 PM	34;37
43	Segunda Revisión de Lectores	3 days?	18/06/18 08:00 AM	20/06/18 05:00 PM	41;42
44	HITO III - AJUSTES	0 days	20/11/17 08:00 AM	20/11/17 08:00 AM	
45	**Evaluación**	3 days?	**21/06/18 08:00 AM**	**23/06/18 05:00 PM**	
46	Calificación del Tribunal Calificador	3 days?	21/06/18 08:00 AM	23/06/18 05:00 PM	40
47	Aprobación de Lectores	3 days?	21/06/18 08:00 AM	23/06/18 05:00 PM	40

Metodología Auditoría TI - página1