ASEGURAMIENTO DE LA INFORMACIÓN EN EL PROCESO TRANSACCIONAL DE RECARGA ELECTRÓNICA DE LA ORGANIZACIÓN FULLCARGA COLOMBIA S.A.

JAIRO YESID MELO MORENO
DANIEL MAURICIO GUTIÉRREZ JAIMES

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES
PROGRAMA DE ADMINISTRACIÓN DE EMPRESAS
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS
BOGOTÁ D.C.
2015

ASEGURAMIENTO DE LA INFORMACIÓN EN EL PROCESO TRANSACCIONAL DE RECARGA ELECTRÓNICA DE LA ORGANIZACIÓN FULLCARGA COLOMBIA S.A.

JAIRO YESID MELO MORENO
DANIEL MAURICIO GUTIÉRREZ JAIMES

DIRECTOR:
WILSON JAVIER CASTRO TORRES

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN GERENCIA DE PROYECTOS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES
PROGRAMA DE ECONOMÍA
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS
BOGOTÁ D.C.
2015

Nota de aceptación

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Fecha: 05 de junio de 2015, Bogotá D.C.

Contenido

TABLA DE ILUSTRACIONES

Págs.

Tabla de anexos

Glosario y siglas

Tabla de glosario y siglas	
***Core* de negocio:**	Es el conjunto de actividades que realiza una empresa y que la caracterizan, definen y diferencian en el mercado.
Data center:	Es una instalación donde se encuentra ubicada una concentración de recursos informáticos para el procesamiento de información de una organización, sea para comunicaciones o almacenamiento de la información.
Host:	Computadora/Servidor conectado a una red que proveen un servicio de ella
ISO:	*International Organization for Standardization.*
PMI:	*Project management institute.*
RTC	Red telefónica conmutada
SGSI:	Sistema de gestión de la seguridad de la información.
SMS:	*Short service message* (mensaje de texto)
TIR:	Tasa interna de retorno
TIRM	Tasa interna de retorno modificada
TPC/IP:	Modelo de descripción de protocolos de red.
TPV:	Terminal punto de venta.
VPN:	Valor presente neto

Resumen ejecutivo

Fullcarga Colombia S.A. es una empresa integradora de servicios transaccionales con el objetivo de ganar participación en el mercado financiero no bancario, para lo cual debe asegurar su operación transaccional.

Con base en lo anterior, se especificó el objetivo de este proyecto en la definición de un plan de diagnóstico e implantación para que Fullcarga Colombia S.A. inicie el proceso de certificación y pueda operar, monitorear, revisar, mantener y mejorar el proceso transaccional de la recarga por medio del sistema de gestión de seguridad de la información alineado a la norma ISO 27001:2005.

La implementación de la ISO 27001:2005 en este proyecto va estar orientado específicamente al proceso de recarga electrónica y a los activos de información que intervienen en este, para dar inicio al proyecto se revisará la documentación general existente en Fullcarga Colombia S.A. y se entregará el plan de trabajo requerido para la implementación del sistema de gestión de seguridad de la información basado en las brechas tecnológicas existentes respecto a la norma ISO 27001:2005 para ir luego en mira de la certificación por medio de ciclos de mejora continua.

Al querer saber cómo se debe realizar el proceso de implementación del SGSI, los estudios realizados en este proyecto dan la conclusión que la mejor opción es realizar un grupo de trabajo interno en la compañía aprovechando la curva de aprendizaje dentro de la compañía y poder generar una cultura de calidad en gestión de seguridad de la información.

Lo anterior orientado a las estrategias de la organización y con el compromiso social de los objetivos establecidos en la declaración del milenio, concretamente el objetivo 8 “el cual se concentra en fomentar una asociación mundial para el desarrollo en donde se medirá el progreso de los países en la materia, este objetivo contempla 6 metas y 16 indicadores" (UN Publications, 2000).

El proyecto ataca fundamentalmente las metas 8A y 8F, la primera busca “desarrollar un sistema comercial y financiero abierto, basado en normas, previsible y no discriminatorio” (UN Publications, 2000) y la segunda, Fullcarga como organización apoyará y dará acceso a los beneficios de las nuevas tecnologías.

PALABRAS CLAVES: Seguridad, plataforma transaccional, recarga electrónica, riesgo, SGSI, Norma ISO 27001:2005.

Introducción

En este proyecto se va a implementar un sistema de gestión de seguridad de la información para que Fullcarga Colombia S.A., como empresa integradora de tecnología de servicios transaccionales requiere de la implementación de un sistema que le permita monitorear, asegurar y controlar los activos de la información a través de herramientas de seguridad que generen un ambiente de confianza en sus clientes y aumente su nivel de competitividad en el mercado.

El proyecto abarca la identificación y reducción de la brecha frente a la norma ISO 27001:2005, por medio de la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) con el objetivo de establecer una economía que garantice mayor nivel de bienestar, empleo y beneficios para sus colaboradores.

Objetivos del trabajo de grado

A continuación se verán los objetivos generales y específicos del trabajo de grado.

1. Objetivo general

Obtener el grado como especialistas en Gerencia de Proyectos.

2. Objetivos específicos

- Establecer entornos de discusión en los fundamentos y diferentes procesos relacionados a la gerencia de Proyectos.
- Desarrollar la investigación en que los ciclos de vida de los proyectos se usan actualmente en la gerencia de proyectos.
- Establecer una referencia entre el conocimiento y la práctica.
- Demostrar los conocimientos adquiridos en el transcurso de la especialización.

1. Formulación

En este capítulo se encuentra la formulación de la situación que está afrontando Fullcarga Colombia S.A. frente a un mercado que se vuelve más exigente en parámetros de calidad y manejo de la información, se puede apreciar como es el antecedente del problema, la empresa, el planteamiento del problema y la mejor solución.

1.1. Antecedentes del problema

Hoy en día el sector privado y público está exigiendo a las compañías fiabilidad, confiabilidad y aseguramiento a las empresas en cuanto se refiere al manejo y procesamiento de información en plataformas electrónicas, es por esto, que se refieren a las entidades de calidad como la ISO que ya tiene unas normas certificables asegurando que las compañías cumplan con estos requisitos mínimos.

Por lo tanto Fullcarga siendo una empresa integradora de tecnología de servicios transaccionales, quiere entrar al mercado de las entidades financieras; sin embargo, este le exige a la compañía estar certificada en la ISO 27001:2005. Esto hace que Fullcarga no pueda adquirir clientes potenciales por requerimientos de mercado y de cumplimiento legal.

1.2. Descripción de la organización

Fullcarga Colombia S.A. es una organización que soportada en una plataforma transaccional propia, realiza operaciones de venta de recarga de líneas celulares, loterías y otros productos virtuales.

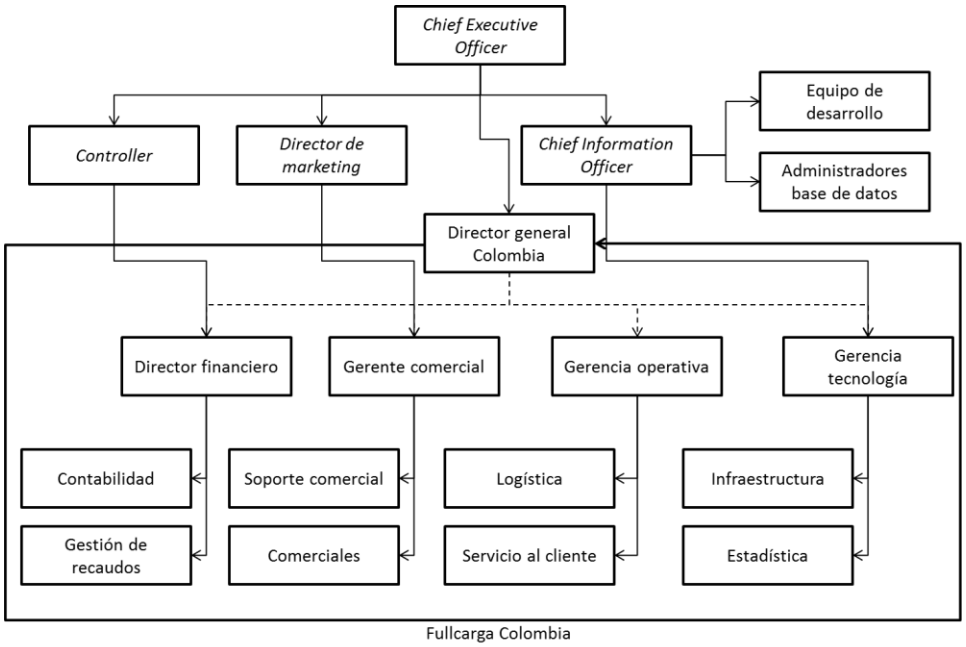
Es considerada, como una de las empresas pioneras en la implantación en Latinoamérica de distribución de productos virtuales.

Desde el año 2004, Fullcarga está implantada en los principales países de Latinoamérica con filiales propias, distribuye recargas para todos los operadores de telefonía de la región y dispone de una extensa red de puntos de venta.

Fullcarga pone a disposición de sus clientes una variedad de soluciones técnicas innovadoras y una estructura de apoyo de posventa, *call center* y profesionales experimentados. Es por ello que la estructura de la organización (ver Ilustración 1) está dirigida principalmente a ofrecer servicios de calidad a sus distribuidores y clientes:

- Transacciones en tiempo real.
- Sistema que garantiza operaciones seguras.
- Disponibilidad 24 horas al día, los 7 días a la semana.
- Plataforma multioperador y multiproducto que permite la venta de diferentes servicios.
- "*Clearing*" de las operaciones financieras garantizado un tiempo adecuado.
- Sin necesidades de inversión por parte de los operadores y clientes.

Ilustración 1. Organigrama de la organización



Fuente: (FullCarga Internacional, 2011)

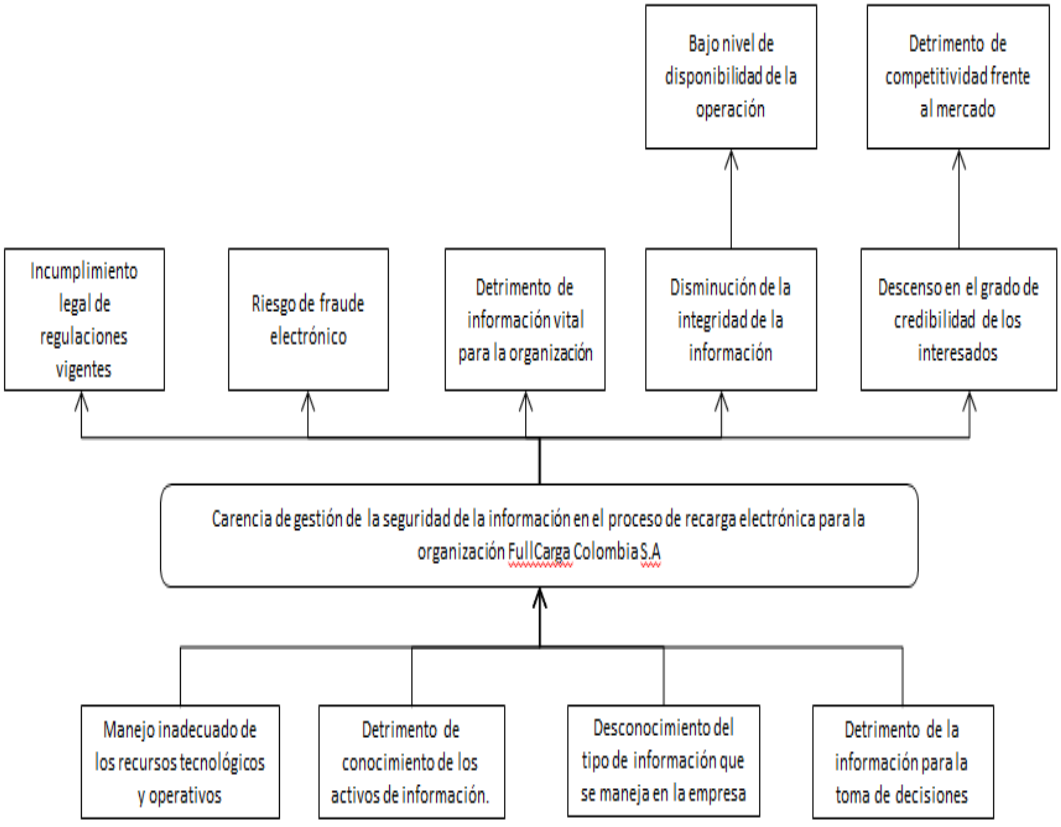
1.3. Planteamiento del problema

A continuación se define las causas y consecuencias del problema que tiene Fullcarga Colombia y los objetivos a los que quiere llegar, planteando el problema de una manera aterrizada.

1.3.1. Árbol de problemas:

En la Ilustración 2 se presentan las causas y consecuencias del problema que tiene Fullcarga Colombia S.A. al no tener un SGSI.

Ilustración 2. Árbol de problemas

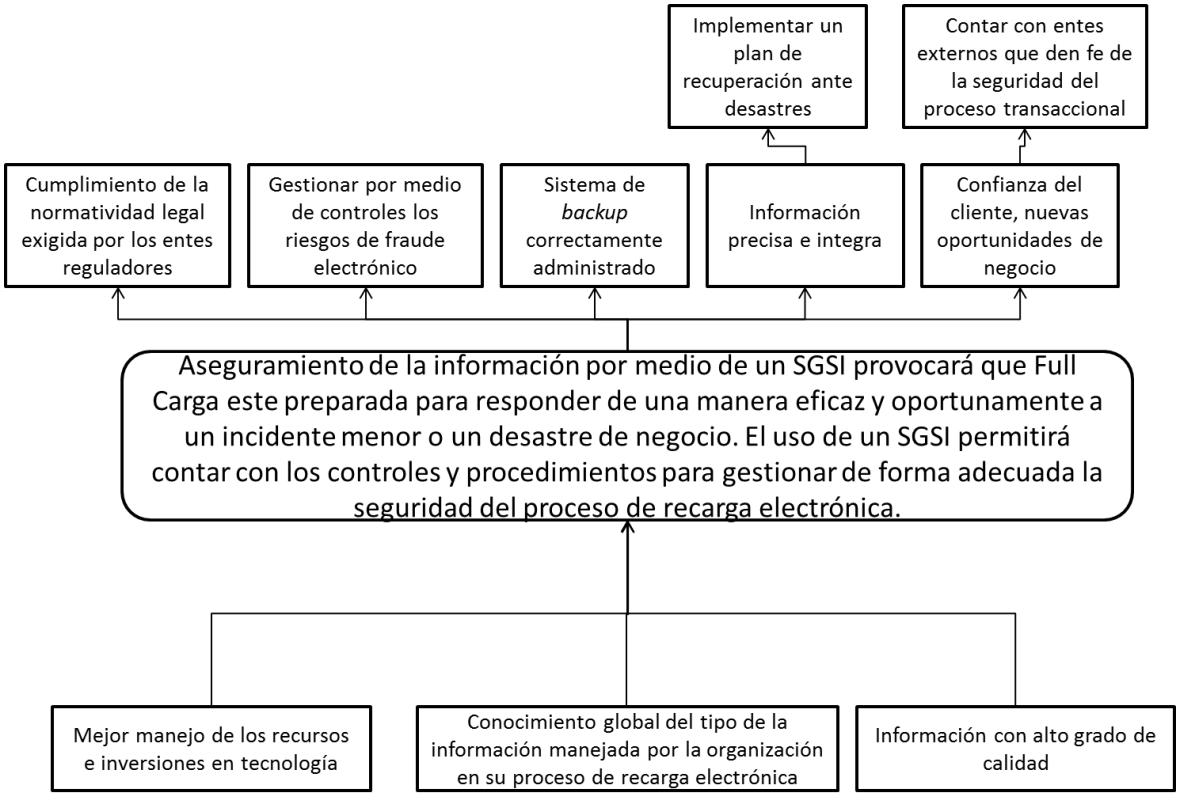


Fuente: Autores del texto

1.3.2. Árbol de objetivos

En la Ilustración 3 se establece el árbol de objetivos, el cual tiene como fin identificar las oportunidades de mejora y objetivos del proyecto.

Ilustración 3. Árbol de objetivos



Fuente: Autores del texto

1.3.3. Descripción principal del problema

La seguridad de la información es el pilar de crecimiento para la organización que basa su *core* de negocio en operaciones virtuales, en donde el cliente tiene como principio trabajar con la organización, siempre que se garantice la seguridad a su información; poder tener la capacidad de responder a eventos inesperados de forma eficiente y eficaz; con la capacidad de resguardar la información clave para la sobrevivencia de la organización, garantizará la estabilidad de la misma.

La implementación de un sistema de gestión de seguridad de la información (SGSI) permitirá conocer la gestión de riesgos existente en la organización y establecer los planes de acción correspondientes que mejoren los controles,

procesos y procedimientos que resguardan la operación; además se podrá establecer directrices claras para la gestión de incidentes de seguridad.

Dado lo anterior, se observa que Fullcarga Colombia S.A. no tiene una guía para manejar los procesos de seguridad de la información en las transacciones de recarga en línea, lo cual genera la necesidad de la certificación del proceso mediante la norma ISO 27001:2005.

Es por esto, que el SGSI está diseñado para proporcionar controles de seguridad que protejan los activos de la información, den confianza a las partes interesadas, incremente la competitividad de la organización y fomenten en los usuarios la importancia de:

- Establecer políticas y objetivos para atender los requerimientos de seguridad de la información de la organización.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear, revisar el desempeño y la efectividad del SGSI.

1.4. Alternativa de solución

Para poder tomar la decisión de la alternativa de solución que fuera las más objetiva para tratar el problema a trabajar, se utilizó la técnica nominal de grupo, la cual muestra como resultado los desarrollos que generen más costos por cambios presentados, el que ajuste más al alcance del proyecto y su continuidad, y ayude a facilitar el diagnóstico del problema.

Las alternativas de solución fueron planteadas por comité primario de Fullcarga Colombia S.A.:

Alternativa 1: Contratar una organización idónea y con la experiencia suficiente para desarrollar el proyecto de certificación del proceso de recarga electrónica.

Alternativa 2: Aprovechar el conocimiento y curva de aprendizaje del personal de Fullcarga Colombia y de éste definir un equipo de trabajo con la dedicación

requerida para el proyecto, capacitarla y luego aplicar lo aprendido desarrollando el proyecto de certificación del proceso de recarga electrónica.

Alternativa 3: Contratar personal nuevo en la compañía dedicado únicamente a la creación del SGSI como un departamento exclusivo y desarrollar los procesos para la certificación del proceso de recarga electrónica.

Utilizando la técnica nominal de grupo (ver

Anexo 1) muestra que la mejor opción es la Alternativa 2, debido a que facilita una utilización del personal en la compañía y su experiencia en los procesos internos.

1.5. Objetivos del proyecto

A continuación se mostraran los objetivos propios del proyecto:

1.5.1. Objetivo general

Implementar un sistema de gestión de seguridad de la información que garantice la integridad, confidencialidad y disponibilidad para todos los activos de información relevantes para la organización, de modo que se asegure la continuidad y entrega de productos y servicios a los interesados con altos estándares de calidad.

1.5.2. Objetivos específicos

- Identificar los controles de seguridad de la información existentes en proceso de recarga electrónica desarrollado en Fullcarga Colombia.
- Definir la brecha de controles de seguridad de la información teniendo en cuenta los controles existes identificados frente a los contenidos en la norma ISO 27001:2005.
- Definir el enfoque de evaluación de riesgo de la organización.
- Establecer las acciones necesarias que den cumplimiento a los controles establecidos en la norma ISO 27001:2005.
- Establecer la documentación requerida para la implementación del SGSI.

2. Estudios y evaluaciones

Se relaciona a continuación los estudios requeridos para establecer la viabilidad del proyecto y tener la base de trabajo y gestión del mismo:

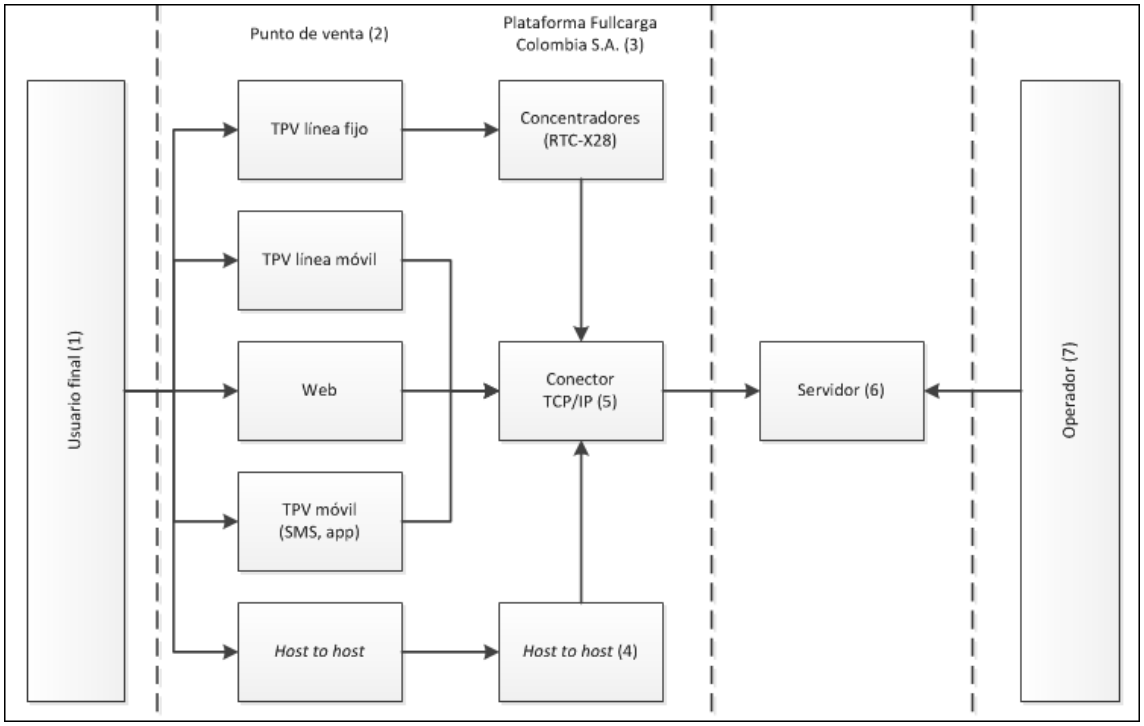
2.1 Estudio técnico

En los estudios técnicos se encuentra la definición al proceso que se va trabajar, la identificación de las normas y guías para un SGSI y su aplicación en el proceso de recarga en línea de Fullcarga Colombia S.A.

2.1.1. Proceso transaccional de recarga electrónica:

A continuación se presenta la descripción del proceso transaccional de recarga electrónica (ver Ilustración 4. Proceso de recarga en línea.), el cual engloba las etapas básicas del proceso de una recarga tanto desde la perspectiva del usuario final como del distribuidor:

Ilustración 4. Proceso de recarga en línea.



Fuente: (FullCarga Internacional, 2011)

El comportamiento del proceso de recarga en línea visto en la Ilustración 4 tiene 7 eventos requeridos para realizar una transacción exitosa; a continuación

(Ilustración 5) se hace la descripción de cada uno de los eventos y roles que hacen en la participación del proceso.

Ilustración 5. Eventos del proceso de carga en línea

Proceso	Descripción del evento
1	El cliente se presenta en uno de los puntos de venta gestión por un distribuidor o mayorista con el objetivo de recargar su teléfono móvil prepago. Para ello, proporciona su número de teléfono, la cantidad a recargar y el nombre del producto deseado.
2	El empleado del punto de venta puede utilizar cualquiera de los métodos disponibles para llevar a cabo la recarga. Es posible utilizar los siguientes dispositivos: • TPV conectado a una línea fija. • TPV móvil. • Dispositivo con conexión a Internet y capacidad de navegación Web. • Teléfono móvil. • Cualquier dispositivo centralizado por un *host* de terceros.
3	La plataforma cuenta con una serie de concentradores capaces de direccionar adecuadamente el tráfico proveniente de todos los TPV de línea fija a través de RTC o X.28 en el formato soportado internamente por el sistema, el cual está basado en el protocolo TCP/IP. Estos concentradores son piezas totalmente modulares que pueden crearse o eliminarse en función de las necesidades existentes en cada implementación.
4	La plataforma admite la reutilización del servicio de recargas por *host* de terceros. De este modo, el número y tipo de dispositivos de recarga es ilimitado, siempre y cuando éstos queden perfectamente centralizados sobre un único equipo servidor, que será quien finalmente interactúe con la plataforma de recargas.
5	Todo el tráfico que entra o sale de la plataforma debe hacerlo sobre el protocolo de comunicaciones TCP/IP. De este modo, la plataforma centraliza todas las peticiones por un único punto y formato, creando a partir de este punto tantos módulos como sea

Proceso	Descripción del evento
	necesario para adaptarse a los protocolos utilizados por los dispositivos de recarga u operadores. En este punto, y siguiendo con la recarga a través del dispositivo seleccionado, tras haberse realizado las concentraciones y conversiones oportunas, la solicitud de recarga llega a la plataforma.
6	La plataforma cuenta con distintos módulos capaces de adaptar el formato de las peticiones recibidas al protocolo utilizado por cada operador. Dichas piezas reciben el nombre de *gateways*. Por ejemplo, el reflejado en la Ilustración 4 se comunica con un operador que utiliza el protocolo ISO 8583. Realizada dicha conversión, la solicitud es remitida al operador. Los *gateways* son piezas clave de cara a integrar la plataforma con cualquier sistema o solución de terceros.
7	El operador recibe la trama de petición y la procesa, como resultado confirma o deniega la solicitud, y remite la respuesta adecuada a la plataforma. Dicha respuesta a su vez será tratada y enviada al dispositivo solicitante, concluyendo así la operativa de recarga. El dispositivo de recarga al recibir la respuesta, imprimirá un ticket de confirmación, se enviará un SMS al usuario final, o en general, dará una respuesta adecuada al empleado del punto de venta y al usuario final. Concluido el proceso se realizará el pago pertinente.

Fuente: (FULLCARGA COLOMBIA S.A., 2012)

2.1.2. Estado del arte

Se puede definir la seguridad informática como un procedimiento que asegura el buen funcionamiento, precaviendo que éste falle, se frustre o se violente, enfocado a proteger la información en procesos de interacción con sistemas digitales y participación de personas.

Teniendo la definición de seguridad informática es importante saber que es un sistema de gestión de seguridad de la información, el cual según (ISO, 2007) lo define como un conjunto de políticas, herramientas y procedimientos cuya finalidad es tener un buen manejo en la administración de la información. A continuación se puede ver los estándares de la seguridad informática y su

principal uso, lo cual hace que se pueda generar un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 27001:2005

La ISO 27001:2005 es el único estándar certificable por parte de la ISO, este estándar cuenta con 39 objetivos de control y 133 controles agrupados en 11 dominios. Al igual que la ISO 9001:2008 se basa en la mejora de un proceso a través del ciclo PHVA (Planear, Hacer, Verificar y Actuar) pero aplicado en el aseguramiento de la información, (ISO, 2007).

ISO 27002, CoBIT, ITIL

La ISO 27002, CoBIT e ITIL son una guía de buenas prácticas para el aseguramiento de la información. Según (ISO/IEC, 2005) la ISO 270002 consiste en identificar un marco de trabajo a través objetivos y controles sugeridos por la organización.

El CoBIT establece un marco de trabajo basado en dominios y procesos, a través del cual se ofrecen unas buenas prácticas enfocadas a optimizar la inversión de recursos en áreas de IT (Borbon Sanabria, 2011).

La ITIL según (Vargas, 2011) es una biblioteca de aseguramiento de la información cuya base de datos está constituida en la mejoras de aseguramiento de la información.

ISO 27005

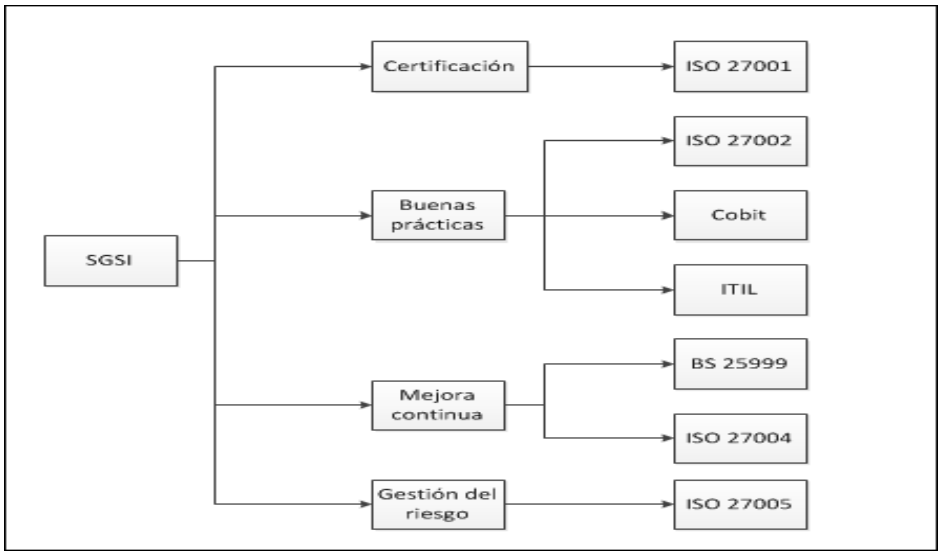
La ISO 27005:2008 provee las pautas para la gestión de riesgos de seguridad de la información, esta guía no es certificable, pero es necesaria para la ISO 27001:2005, debido a que es el plan de acción para repuestas en aseguramiento de la información, (ISO, 2008).

BS 25999 e ISO 27004

LA BS25999 al igual que ISO 27004 (Marblestation, 2008) son estándares de mejora continua cuando el proceso de aseguramiento de la información ya se encuentra establecido y ejecutándose para dar la continuidad del negocio.

A continuación en la Ilustración 6 se observa la interacción que hay en el estado del arte y la funcionalidad de cada uno de estos.

Ilustración 6. Interacción estado del arte

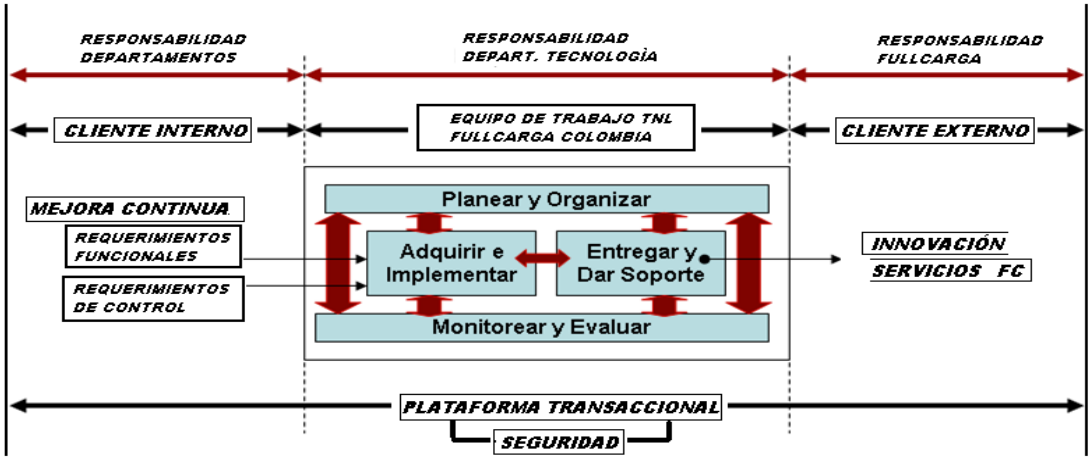


Fuente: Autores del texto.

2.1.3. Aplicación del estado del arte – Diseño conceptual

Actualmente Fullcarga tiene un modelo según los estándares de CoBIT para el proceso de recarga en línea (Ilustración 7) el cual se puede representar de la siguiente manera:

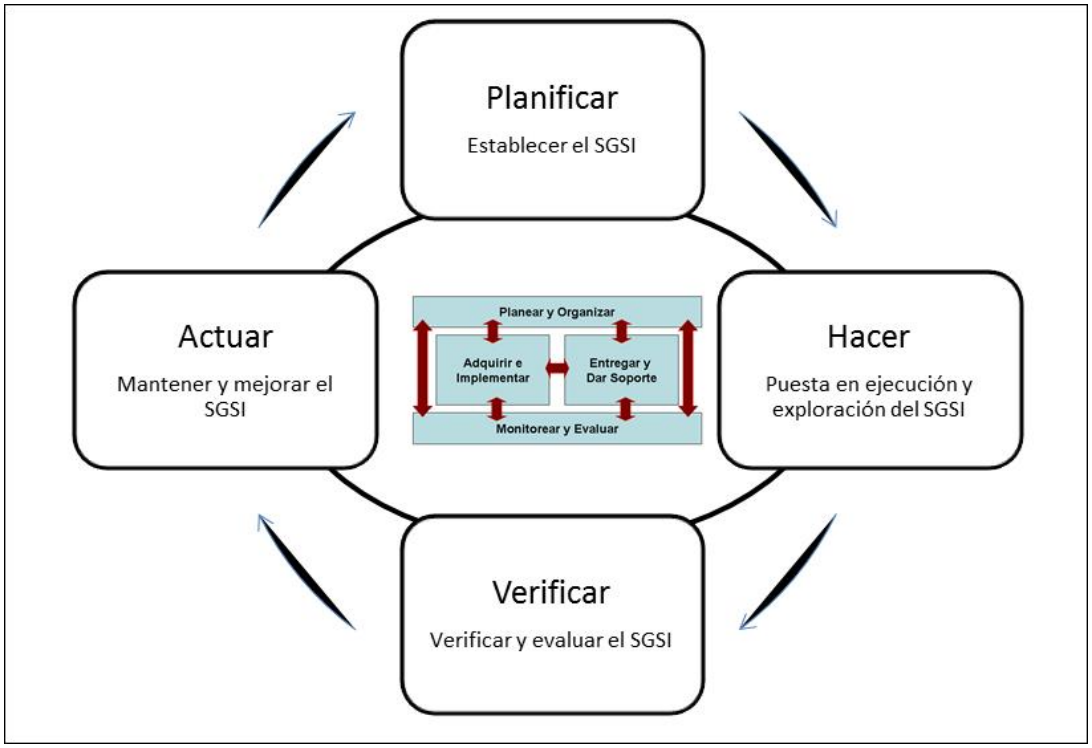
Ilustración 7. Modelo actual de Fullcarga Colombia S.A.



Fuente: (FULLCARGA COLOMBIA S.A., 2012)

Lo que se quiere es aplicar el estándar ISO 27001:2005 con base a la metodología ciclo de *Deming* para iniciar el proceso de certificación, teniendo el modelo mejorado del proceso de recarga en línea (Ilustración 8) de la siguiente manera:

Ilustración 8. Modelo mejorado de SGSI del proceso de recarga en línea



Fuente: Autores del texto

Para identificar el estado de Fullcarga Colombia S.A. en el proceso de recarga en línea frente a la ISO 27001:2005 se realiza un “FORMULARIO PARA AUTODIAGNÓSTICO DE SEGURIDAD FULLCARGA COLOMBIA” con base a la ISO 27001 (Anexo 5), y adicionalmente se realiza matriz de mapeo de normatividad según la “circular 052” (Anexo 6).

2.2 Estudio de sostenibilidad

Los estudios de sostenibilidad muestran la viabilidad del proyecto legalmente, socialmente, económicamente y ambientalmente, lo cual son factores de decisión que permiten actuar en proceder o parar el proyecto si no es sostenible.

2.2.1. Legal

Para que este proyecto sea sostenible legalmente se debe cumplir la ley 1273 de 2009 de la constitución Colombiana, la cual comunica de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; es por esto que se debe realizar el aseguramiento de la calidad, y cualquier infracción a esta ley puede generar no solo la terminación de proyecto, sino la liquidación de la compañía.

2.2.2. Social

Con el proyecto se busca cubrir la necesidad de inclusión financiera, establecida como cumplimiento de ley a las entidades financieras por el Gonierno Nacional, y que Fullcarga ha establecido dentro de sus prioridades estratégicas al contar con los puntos en zonas estratégicas que suplen esta necesidad; con la implementación del sistema de seguridad de la información, la organización lograra ingresar como corresponsal bancario, en donde se acercará al usuario financiero de sectores populares y residenciales, por medio de un canal de fácil acceso a la actividad financiera.

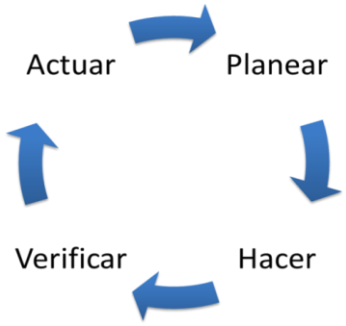
2.2.3. Ambiental

La sostenibilidad ambiental identifica el ciclo de vida del proyecto y el impacto ambiental que tiene el proyecto mediante eco-indicadores, como se puede ver a continuación.

2.2.3.1. Análisis ciclo de vida.

La evaluación del ciclo de vida (ECV) se basó en la metodología de la ISO 14040:2006, en donde se evaluó los aspectos ambientales y los impactos potenciales asociados al proyecto. En donde el alcance del proyecto enmarcado en la ISO 27001:2005 cumple un ciclo PHVA (Planear – Hacer – Verificar – Actuar) como se puede ver en la Ilustración 9.

Ilustración 9. Ciclo PHVA



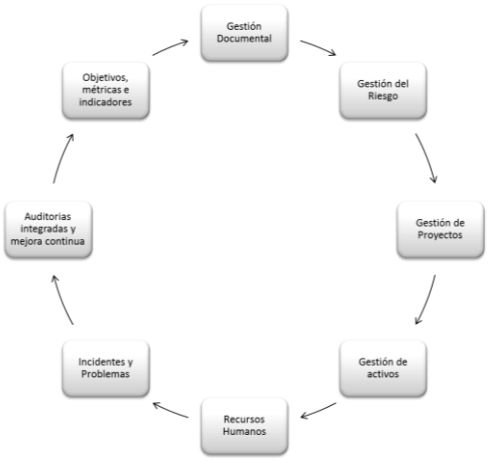
Fuente: Autores del texto

Se define a continuación cada etapa del ciclo del proyecto:

- Planear: se define las metas, los métodos para cumplirlas y las capacitaciones. Se realizan las acciones preventivas.
- Hacer: se realiza el trabajo planeado.
- Verificar: se evalua lo ejecutado mediante indicadores cuantitativos y cualitativos.
- Actuar: se analiza los resultados de la verificación y eliminar o reducir las no conformidades. Se realizan las acciones correctivas.

Por lo tanto se define el ciclo de vida para un SGSI de la siguiente manera (Ilustración 10):

Ilustración 10. Ciclo de vida ISO 27001



Fuente: (GES CONSULTOR, 2013)

2.2.3.2. Eco-indicadores.

Se utilizaran en el proyecto los eco-indicadores 99 que se clasifican (Ilustración 11) de la siguiente manera para poder hacer un análisis al ciclo de vida del proyecto:

Ilustración 11 Valores estándar de eco-Indicador 99

Materiales	Medida de 1 kilo de material.
Procesos de producción	Tratamiento y procesado de varios materiales. Cada tratamiento se expresa en la unidad apropiada al proceso particular (metros cuadrados, kilos, metros soldados, etc.)
Procesos de transporte	No aplican para el proyecto.
Procesos de generación de energía	Se determinan unidades para electricidad y calor.
Escenarios de eliminación	Se determinan unidades para electricidad y calor.

Fuente: (Goedkoop, Effting, & Collignon, 1999)

Como base para el proyecto utilizamos el “punto eco-indicador” (Pt) como medida para el proyecto.

Para definir los parámetros de los ecos-indicadores del proyecto y su equivalencia se toma como base la Ilustración 12.

Ilustración 12 Equivalencia de Eco puntos

Material	**Cantidad**	**Total eco-puntos**
Papel blanco	400 Kg	1
Papel reciclado	100 Kg	2
Energía	1.000 KW	1

Fuente: (Goedkoop, Effting, & Collignon, 1999).

Para este proyecto se tiene en cuenta los parámetros de generación de energía y utilización de papel como se ve en la Ilustración 13.

Ilustración 13 Simulación eco-Indicadores

Material	Cantidad	Consumo en KW mes	Eco puntos	Mili eco puntos
Computadores	3	0,6	0,0006	0,6
Lámpara	4	0,16	0,00016	0,16
Impresora laser	2	0,3	0,0003	0,3
Papel reciclado	1	10 Kg	0,01	10
Papel blanco	1	5 Kg	0,05	50
		Total	0,06106	61,06

Fuente: (Ministerio de Minas y Energía de Perú, 2010)

2.2.4. Económica

La identificación de sostenibilidad económica del proyecto se realiza calculando las entradas y salidas de capital del proyecto, en periodos iguales (1 mes durante 8 meses) para la ejecución del SGSI y se proyecto durante tres años la penetración al mercando que hace la compañía queriendo activas sus 2.000 puntos transaccionales listos para que puedan responder como corresponsal bancario, identificando variables de inversión como la tasa interna de retorno (TIR), el valor nominal anual (VNA) y la tasa interna de retorno modificada (TIRM).

Para ver más detalle de este análisis, ver capítulo 2.3 Estudio financiero. Dado a la naturaleza del proyecto que es endógeno de una compañía para su mejora y mejor posicionamiento en el mercado frente a la competencia, se habla de una inversión de un valor de COP$142.995.216 de presupuesto frente a una tasa interna de retorno de 20,40%, comparando contra un presupuesto inicial de COP$150.000.000. Adicionalmente genera un conocimiento más preciso de los niveles de satisfacción alcanzados en las actividades y procesos de negocio ayuda, además, a introducir cambios con una mayor garantía en los resultados

que se desean obtener y reduce el nivel de incertidumbre y de posibles pérdidas económicas debido a decisiones comprometidas.

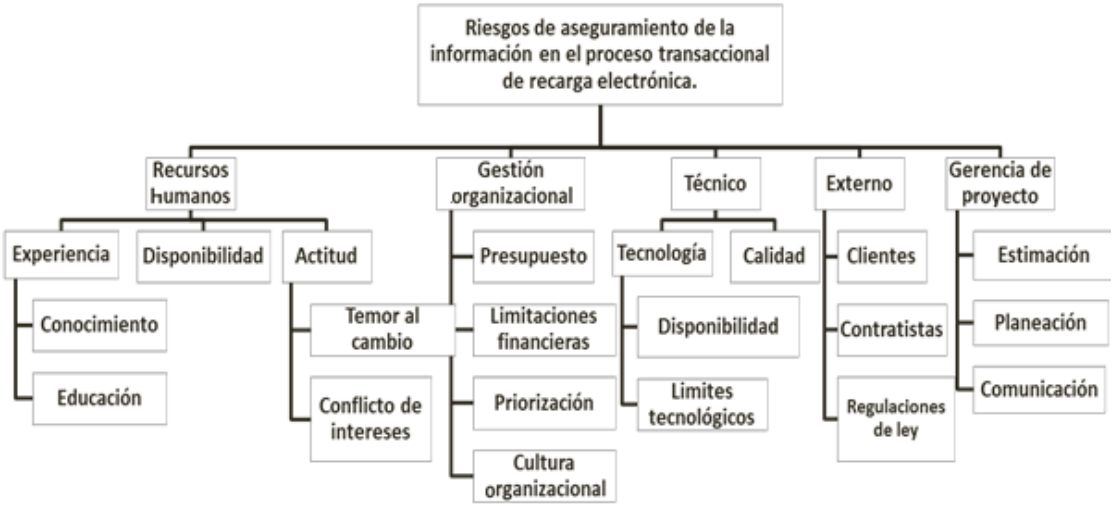
2.2.5. Riesgos

El riesgo es la probabilidad de que en el proyecto se realice atrasos, sobrecostos e inclusive abandono el proyecto, en esta sección se identifica estos riesgos y los involucrados para saber qué rol es el que tienen en el proyecto.

2.2.5.1. *Risk Breakdown Structure*

Se identifican los riesgos en la Ilustración 14 que pueden afectar al proyecto al momento de planear e implementar un sistema de gestión de seguridad de la Información.

Ilustración 14. ReBS



Fuente: Autores del texto

2.2.5.2. Involucrados

Es importante identificar los involucrados del proyecto y los roles que juegan estos; se observa a continuación, en la Ilustración 15, el cuadro de interesados en el proyecto identificando cuales son beneficiados, excluidos o perjudicados.

Ilustración 15. Cuadro de interesados

Beneficiarios Directos	**Beneficiarios indirectos**
Patrocinador (C.I.O)	Cadena comercial (mayoristas - distribuidores)
Directores del proyecto	C.E.O
Equipo del proyecto	Socios
Equipo departamento de tecnología	Clientes finales

Excluidos Neutrales	**Perjudicados**
Comité primario Fullcarga Colombia	Competencia
Operadores/proveedores del producto	Entidades reguladoras
Proveedores de servicios de *data center*	

Fuente: Autores del texto

A continuación se identifica los involucrados directamente al proyecto y el Rol qué hace este en él, como se puede observar en la Tabla 16.

Tabla 16. Registro de interesados

Nombre / Entidad		Posición en la organización	Ubicación	Rol en el proyecto
1. Patrocinador (C.I.O)	Beatriz Brum	*Chief Information Officer*	Zaragoza - España	Patrocinador
2. Directores del proyecto	Jairo Melo	Jefe de tecnología Colombia	Bogotá - Colombia	Gerente de proyecto
3. Equipo del proyecto	Eder Montalvo Rubén Corral Lucio Núñez Daniel Gutiérrez Mónica Chaparro	Soporte Infraestructura Soporte aplicaciones DBA Externo	Bogotá - Colombia Zaragoza - España Buenos Aires - Arg Bogotá - Colombia Bogotá - Colombia	Equipo de proyecto
4. Equipo departamento de tecnología	Departamento de tecnología: Desarrollo / Pruebas / TI Local /Soporte	Implementación, pruebas, entrega, soporte de las herramientas tecnológicas de la organización	Colombia Argentina España	Personal de implementación de los correctivos y controles que apliquen luego de definir el gap respecto

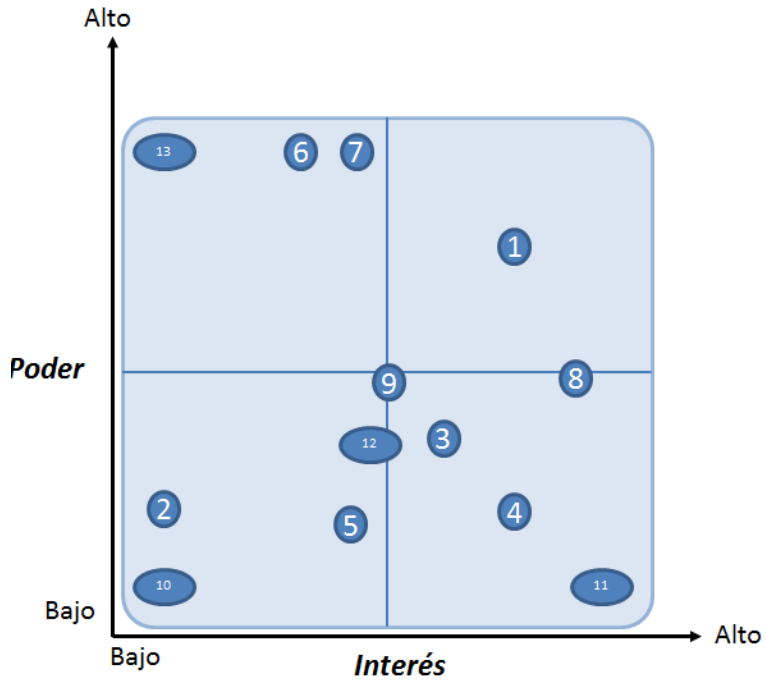
Nombre / Entidad		Posición en la organización	Ubicación	Rol en el proyecto
				a la norma 27001 y el plan de acción
5. Cadena comercial	Mayoristas – Distribuidores	Socios de negocio, son el soporte directo a nivel comercial del punto de venta.	Bogotá - Colombia	
6. C.E.O	Gonzalo Sacristán	*Chief Executive Officer*	Bilbao – España	
7. Socios	Socios mesa directiva	Socios mesa directiva	Colombia - España	
8. Clientes finales	Cliente finales	Puntos de venta, en donde se ubican los POS, punto de partida de las transacciones.	Bogotá - Colombia	
9. Comité primario	Comité primario Fullcarga Colombia	Nivel gerencia de Fullcarga Colombia- Gerencias de los	Bogotá - Colombia	

Nombre / Entidad		Posición en la organización	Ubicación	Rol en el proyecto
Fullcarga Colombia		diferentes departamentos.		
10 Operadores / proveedores de productos comercializados	Comcel, Movistar, Tigo, Une, Uff, Etb, Avantel, Directv, entidades financieras y Loticolombia	Proveedor productos	Colombia	
11. Proveedores de servicios de *datacenter*	Telmex	Proveedores servicios	Colombia	
12. Competencia	Movilred S.A., Solida S.A., Punto Naranja S.A., *Movilway* S.A.,	Competencia	Bogotá - Colombia	
13. Entidades reguladoras	Superintendencia de sociedades Superintendencia financiera Ministerio de comunicaciones	Entidades reguladoras	Bogotá - Colombia	

Fuente: Autores del texto

La Matriz de poder/influencia muestra la importancia de los interesados en el proyecto al momento de tomar una decisión, en la Ilustración 17 se identifica el poder e interés de cada uno de los involucrados en el proyecto.

Ilustración 17. Gráfica de poder e interés



Fuente: Autores del texto.

En la Ilustración 18 se lista cada uno de los interesados que tienen poder e interés en el proyecto.

Ilustración 18. Tabla de poder e interés

1. Patrocinador (C.I.O)	2. Directores del proyecto	3. Equipo del proyecto	4. Equipo departamento de tecnología	5. Cadena comercial
6. C.E.O	7. Socios	8. Clientes finales	9. Comité primario Fullcarga Colombia	10 Operadores / proveedores de productos comercializados
11. Proveedores de servicios de datacenter	12. Competencia	13. Entidades reguladoras		

Fuente: Autores del texto

Para la administración de los involucrados en el proyecto se debe crear inicialmente un perfil de cada uno y según su nivel de poder interés se dirige a

la comunicación. Toda comunicación tiene que ser por escrita (vía correo electrónico), si se comunicó una información o se tomaron decisiones verbalmente hay que escribir el correo como constancia de lo que se habló. Resolver los desacuerdos que se encuentre con los involucrados, negociar esos desacuerdos para el bien del proyecto y dar la solución para poder obtener el alcance.

2.2.5.3. Análisis cualitativo y cuantitativo

A continuación (Ilustración 19) se mostrará el análisis cuantitativo y cualitativo de los riesgos relacionados con el desarrollo del proyecto.

Ilustración 19 Análisis cuantitativo y cualitativo de riesgos

Id.	Descripción del riesgo	Tipo de riesgo	Prob. de ocurrencia	Impacto	Evaluación del riesgo
R01	Cambios en los requisitos	Producto	20	4	0,8
R02	Bajas en el equipo de desarrollo	Proyecto	30	4	1,2
R03	Falta de experiencia en tareas de planificación	Proyecto	50	2	1
R04	Falta de experiencia con las herramientas utilizadas	Proyecto	50	2	1
R05	Diseño erróneo	Producto	40	3	1,2
R06	Falta de un experto	Proyecto	80	1	0,8
R07	Pérdida de documentación y/o otros artefactos	Proyecto	40	4	1,6
R08	Conflictos entre los integrantes del grupo	Proyecto	75	2	1,5
R09	Inestabilidad del entorno de desarrollo y documentación el proyecto	Proyecto	80	5	4
R10	Mala estimación de costos	Proyecto	50	3	1,5
R11	Falta de seguimiento de tareas	Proyecto	50	3	1,5
R12	Falta de comunicación entre los integrantes	Proyecto	20	2	0,4

Fuente: Autores del texto

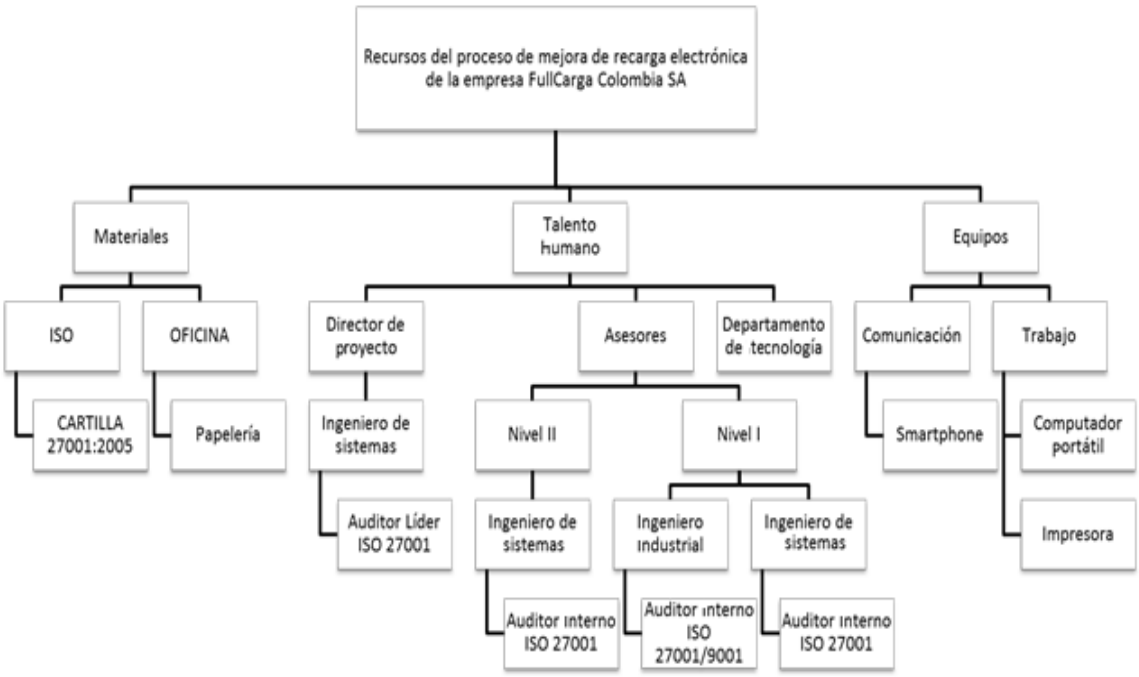
2.3 Estudio financiero

El objetivo del estudio financiero es sistematizar la información que se ha estado trabajando en este proyecto y llevarla a recursos monetarios. Como se puede ver a continuación.

2.3.1. *Resource breakdown structure* – ReBS

A continuación en la Ilustración 20 se puede detallar la estructura de recursos necesarios para poder ejecutar el proyecto.

Ilustración 20. *Resource breakdown structure*

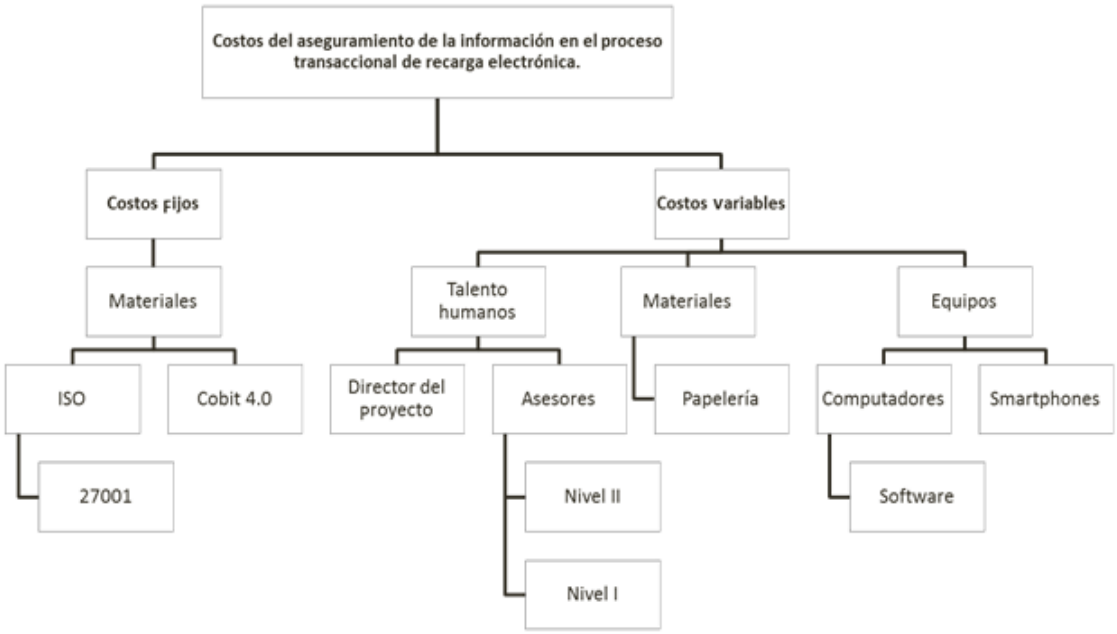


Fuente: Autores del texto

2.3.2. *Cost breakdown structure* –CBS-

En la Ilustración 21 se podrá observar el desglose de la estructura de costos del proyecto identificando sus costos fijos y variables.

Ilustración 21 *Cost breakdown structure*



Fuente: Autores del texto

2.3.3. Caso de negocio y presupuesto

Los costos del proyecto se calcularon con base en el tiempo estimado que tomará realizar el mismo según el alcance indicado y los recursos requeridos.

Dadas las exigencias del proyecto se debe tener en cuenta la capacitación del equipo de trabajo dentro de los costos del proyecto.

Es de importancia aclarar, que luego de definir la carta de aplicabilidad se deberán implementar cambios para cumplir la norma y lograr la certificación, esto podrá generar costos adicionales, los cuales se aproximan en un caso de negocio global cuyo proyecto tiene tres fases, 1. Diagnóstico, 2. Implementación y 3. Certificación por un valor estimado de COP $2.500.000.000.

Los honorarios estimados para la realización del proyecto en la fase de diagnóstico (Ilustración 22), tomando como base el equipo de trabajo propuesto serán de: COP $ 150.000.000.

Ilustración 22 Presupuesto estimado EDT

EDT	Descripción	Presupuesto
1	Implementación sistema de gestión de seguridad de la información para el proceso de recarga electrónica en Fullcarga Colombia	$ 150.000.000
1.1	Diseño del SGSI	**$ 7.500.000**
1.1.1	Definición del SGSI	$ 2.500.000
1.1.2	Definición de fundamentos del SGSI	$ 5.000.000
1.2	Diagnóstico del SGSI	**$ 23.000.000**
1.2.1	Carta de aplicabilidad SGSI	$ 3.000.000
1.2.2	Análisis de riesgo	$ 20.000.000
1.3	Implementación del SGSI	**$ 22.000.000**
1.3.1	Organización de la seguridad de la información	$ 20.000.000
1.3.2	Políticas de seguridad	$ 2.000.000
1.4	Capacitación	**$ 27.500.000**
1.4.1	Formación y entrenamiento	$ 25.000.000
1.4.2	Definición del calendario de formación y entrenamientos	$ 1.000.000
1.4.3	Preparación del material de formación y entrenamiento	$ 1.500.000
1.5	Gerencia de proyectos	$ 70.000.000

Fuente: Autores del texto

2.3.4. Fuentes y usos de fondos

Los datos a continuación en la Ilustración 23 corresponden a los ingresos y egresos estimados que tendrá el proyecto en cada sus periodos.

Ilustración 23 Fuentes y usos del proyecto

	Mes 0	Mes 1	Mes 2	Mes 3	Mes 4
Fuentes					
Caja	$ 19.098.800,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00
Financiación	$ -	$ -	$ -	$ -	$ -
Total fuentes	$ 19.098.800,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00
Usos					
Computadores	$ 7.200.000,00	$ -	$ -	$ -	$ -
Celulares	$ 1.050.000,00	$ -	$ -	$ -	$ -
Software	$ 1.523.200,00	$ -	$ -	$ -	$ -
Curso de Auditoria Interna Norma ISO 27001	$ 3.858.933,33	$ -	$ -	$ -	$ -
Curso Auditor líder	$ 5.084.666,67	$ -	$ -	$ -	$ -
Cartilla ISO27001:2005 [CHF $134]	$ 245.000,00	$ -	$ -	$ -	$ -
Elementos de oficina (papelería) y generales	$ 137.000,00	$ 150.000,00	$ 150.000,00	$ 150.000,00	$ 150.000,00
Nómina	$ -	$ 15.337.052,00	$ 15.337.052,00	$ 15.337.052,00	$ 15.337.052,00
Total Usos	$ 19.098.800,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00

	Mes 5	Mes 6	Mes 7	Mes 8
Fuentes				
Caja	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00
Financiación	$ -	$ -	$ -	$ -
Total fuentes	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00
Usos				
Computadores	$ -	$ -	$ -	$ -
Celulares	$ -	$ -	$ -	$ -
Software	$ -	$ -	$ -	$ -
Curso de Auditoria Interna Norma ISO 27001	$ -	$ -	$ -	$ -
Curso Auditor líder	$ -	$ -	$ -	$ -
Cartilla ISO27001:2005 [CHF $134]	$ -	$ -	$ -	$ -
Elementos de oficina (papelería) y generales	$ 150.000,00	$ 150.000,00	$ 150.000,00	$ 150.000,00
Nómina	$ 15.337.052,00	$ 15.337.052,00	$ 15.337.052,00	$ 15.337.052,00
Total Usos	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00	$ 15.487.052,00

Fuente: Autores del texto

2.3.5. Flujo de caja

A continuación se lista los datos del flujo de caja del proyecto, basados en la necesidad del proyecto:

Cuadro de pre inversión:

Los datos relacionados en la Ilustración 24, corresponden a la identificación de necesidades básicas requeridas para el inicio del proyecto, como es el caso de capacitación de un auditor líder que garantice la prestación del servicio y

aumente la competitividad de los servicios a ofrecer y la capacitación de la auditoria interna.

Ilustración 24. Cuadro de pre Inversión

PREINVERSIÓN				
CONCEPTO	UNIDAD DE MEDIDA	VALOR	CANT	TOTAL
Curso de auditoria interna Norma ISO 27001	Global	$ 3.858.933,33	1	$ 3.858.933,33
Curso auditor líder	Global	$ 5.084.666,67	1	$ 5.084.666,67
Cartilla ISO27001:2005 [CHF $134]	Unidad	$ 245.000,00	1	$ 245.000,00
Elementos de oficina (papelería) y generales	Mensual	$ 137.000,00	1	$ 137.000,00
		TOTAL		9.325.600,00

Fuente: Autores del texto.

Cuadro de inversión técnica

En la Ilustración 25 se relacionan los recursos técnicos a utilizar en el desempeño de los trabajos.

Ilustración 25. Cuadro de inversión técnica

INVERSIÓN TÉCNICA				
CONCEPTO	UND MEDIDA	VALOR	CANT	TOTAL
Computadores (ultrabook HP folio 13 - Corei5 - 4 Gb - 128 Gb disco en estado solido)	unidad	1.800.000,00	4,00	7.200.000,00
Celulares (BlackBerry 8520 prepago Comcel)	unidad	350.000,00	3,00	1.050.000,00
Software (office PYME)	Paquete x 3	1.523.200,00	1,00	1.523.200,00
		TOTAL		9.773.200,00

Fuente: Autores del texto.

Cuadro de inversión operativa

En la Ilustración 26 se identifica los costos mensuales operativos para que se pueda generar el proyecto, como se ven a continuación:

Ilustración 26. Cuadro de inversión operativa

INVERSIÓN OPERATIVA				
CONCEPTO	UNIDAD DE MEDIDA	VALOR	CANT	TOTAL
Nómina	Mensual	$ 15.337.052,00	1	$ 15.337.052,00
		SUBTOTAL		15.337.052,00

Otros	UNIDAD DE MEDIDA	VALOR	CANT	TOTAL
Elementos de oficina (papelería) y generales	Mensual	$ 150.000,00	1	$ 150.000,00
		SUBTOTAL		150.000,00

INVERSIÓN OPERATIVA TOTAL	15.487.052,00

Fuente: Autores del texto

Flujo de fondo libre

En la Ilustración 27 se puede observar el flujo de fondo libre del proyecto, el cual tiene dos fases, la primera es la realización del proyecto del SGSI que tiene un tiempo de 8 meses. Para proyectar los ingresos después del proyecto, la empresa busca abarcar al menos el 4% del mercado actual de corresponsales bancarios que se encuentran en el país según el reporte de inclusión financiera (Superintendencia Financiera de Colombia, 2014) en los siguientes 3 años, el cual de los 40.000 puntos de recarga electrónica que tiene en todo el país la compañía, tienen 2.000 puntos listos que cumplen la normatividad de corresponsal bancario, pero se iniciarían con 800 puntos con una tasa de crecimiento del 2.5% mensual.

Ilustración 27. Cuadro flujo de fondo libre

Concepto	Mes 0	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Preinversión	9.325.600	-	-	-	-	-	-	-	-
Inversión técnica	9.773.200	-	-	-	-	-	-	-	-
Ingresos									
Costos	-	15.337.052	15.337.052	15.337.052	15.337.052	15.337.052	15.337.052	15.337.052	15.337.052
Gastos	-	150.000	150.000	150.000	150.000	150.000	150.000	150.000	150.000
Total	**(19.098.800)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**	**(15.487.052)**

Concepto	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13	Mes 14	Mes 15	Mes 16	Mes 17
Preinversión	-	-	-	-	-	-	-	-	-
Inversión técnica	-	-	-	-	-	-	-	-	-
Ingresos	61.676.935	63.218.858	64.837.878	66.456.897	68.153.013	69.849.129	71.622.341	73.395.552	75.245.861
Costos	-	-	-	-	-	-	-	-	-
Gastos	-	-	-	-	-	-	-	-	-
Total	**61.676.935**	**63.218.858**	**64.837.878**	**66.456.897**	**68.153.013**	**69.849.129**	**71.622.341**	**73.395.552**	**75.245.861**

Concepto	Mes 18	Mes 19	Mes 20	Mes 21	Mes 22	Mes 23	Mes 24	Mes 25	Mes 26
Preinversión	-	-	-	-	-	-	-	-	-
Inversión técnica	-	-	-	-	-	-	-	-	-
Ingresos	77.096.169	79.023.573	81.028.073	83.032.574	85.114.170	87.272.863	89.431.556	91.667.344	93.980.229
Costos	-	-	-	-	-	-	-	-	-
Gastos	-	-	-	-	-	-	-	-	-
Total	**77.096.169**	**79.023.573**	**81.028.073**	**83.032.574**	**85.114.170**	**87.272.863**	**89.431.556**	**91.667.344**	**93.980.229**

Concepto	Mes 27	Mes 28	Mes 29	Mes 30	Mes 31	Mes 32	Mes 33	Mes 34	Mes 35
Preinversión	-	-	-	-	-	-	-	-	-
Inversión técnica	-	-	-	-	-	-	-	-	-
Ingresos	96.293.115	98.683.096	101.150.173	103.694.347	106.315.616	108.936.886	111.635.252	114.410.714	117.263.272
Costos	-	-	-	-	-	-	-	-	-
Gastos	-	-	-	-	-	-	-	-	-
Total	**96.293.115**	**98.683.096**	**101.150.173**	**103.694.347**	**106.315.616**	**108.936.886**	**111.635.252**	**114.410.714**	**117.263.272**

Concepto	Mes 36	Mes 37	Mes 38	Mes 39	Mes 40	Mes 41	Mes 42	Mes 43	Mes 44
Preinversión	-	-	-	-	-	-	-	-	-
Inversión técnica	-	-	-	-	-	-	-	-	-
Ingresos	120.192.927	123.199.677	126.283.524	129.444.467	132.682.506	135.997.641	139.389.873	142.859.200	146.405.624
Costos	-	-	-	-	-	-	-	-	-
Gastos	-	-	-	-	-	-	-	-	-
Total	**120.192.927**	**123.199.677**	**126.283.524**	**129.444.467**	**132.682.506**	**135.997.641**	**139.389.873**	**142.859.200**	**146.405.624**

Fuente: Autores del texto

2.3.6. Evaluación financiera

Con el cuadro de flujo de fondo libre (Ilustración 27) se calcularon los indicadores de evaluación financiera para saber la factibilidad y rentabilidad del proyecto. Dando los siguientes resultados (Ilustración 28):

Ilustración 28. Indicadores evaluación financiera

Concepto	Valor
TIR	20,40%
VNA	229.106.315
TIO	10,00%
TIRM	13,85%

Fuente: Autores del texto

Concluyendo lo siguiente:

- La evaluación financiera del proyecto da como resultado que a una tasa de oportunidad de inversión del 20,42% (TIR) el proyecto se hace rentable cuando el costo interno de oportunidad es menor.
- Con una tasa interna de retorno de 10% de acuerdo a un estudio del Banco de la Republica (Banco de la Republica de Colombia, 2006) hace que el valor presente neto sea $229.106.315 (Doscientos veinte y nueve millones ciento seis mel trescientos quince pesos mcte) haciento que la invensión del SGSI tenga una rentabilidad futuro beneficiosa para la compañía.
- La TIR de 20,40% indica la tasa máxima para apalancamiento financiero para que el proyecto tenga un cubrimiento de la preinversión.
- La TIRM de 13,85% se da con una tasa financiera de 20,40% y una tasa de re inversión de 10% la cual hace la nueva tasa máxima para un nuevo apalancamiento financiero.

2.3.7. Análisis de sensibilidad

A continuación se relaciona los análisis de sensibilidad del proyecto:

A. Financiero

Se realiza dos escenarios en donde el proyecto va a generar una tasa de reinversión, también denominada como costo de oportunidad, e identificar la viabilidad del proyecto según su valor presente neto. Con una tasa de oportunidad de 5%, la TIR y 8% (ver Ilustración 29)

Ilustración 29 Análisis de sensibilidad financiero

Concepto	Valor	Valor	Valor
TIR	7,52%	7,52%	7,52%
VNA	$ 1.895.549,66	$ 0,00	($ 322.051,81)
COSTO DE OPORTUNIDAD	5%	7,52%	8%

Fuente: Autores del texto

Se observa que si el proyecto fuera patrocinado por una persona que busca una reinversión, debe tener un costo de oportunidad menor que la TIR para generar ganancias.

B. Operativo

Para poder hacer el análisis de sensibilidad operativo es necesario enfocarse en el centro de costos del proyecto, y es en la nómina, por lo tanto se realiza el supuesto de la contratación de los asesores nivel I, como prestación de servicios por la duración del proyecto con salarios de COP$2.000.000 mensuales, y se obtiene los resultados presentados en la Ilustración 30.

Ilustración 30 Análisis de sensibilidad operativo

	Proyecto V1	Proyecto V2
Concepto	Valor	Valor
TIR	7,52%	18,31%
TIRM	6,31%	11,36%
VNA	$ 0,00	($ 0,00)
COSTO DE OPORTUNIDAD	5%	5%

Fuente: Autores del texto

Teniendo la conclusión que el proyecto se vuelve más atractivo para los inversionistas. Si se realiza los cambios de tipo de contratación para los asesores nivel I.

C. Comparación de dos proyectos mutuamente excluyentes

A continuación (Ilustración 31) se hace la comparación de las dos alternativas de solución del proyecto el cual se hace repartición de costos durante 8 meses según el proyecto, el primer escenario es el evaluado inicialmente utilizando personal de la compañía para diagnosticar, implementar y controlar el SGSI y el segundo escenario es contratar una empresa de consultoría especializada en SGSI.

Ilustración 31 Escenarios de proyectos

Escenario 1									
Concepto	0	1	2	3	4	5	6	7	8
Preinversión	$ 9.325.600								
Inversión Técnica	$ 9.773.200								
Costos		$ 15.337.052	$ 15.337.052	$ 15.337.052	$ 15.337.052	$ 15.337.052	$ 15.337.052	$ 15.337.052	$ 15.337.052
Gastos		$ 150.000	$ 150.000	$ 150.000	$ 150.000	$ 150.000	$ 150.000	$ 150.000	$ 150.000
Total Acumulado	$ 19.098.800	$ 34.585.852	$ 50.072.904	$ 65.559.956	$ 81.047.008	$ 96.534.060	$ 112.021.112	$ 127.508.164	$ 142.995.216

Escenario 2									
Concepto	0	1	2	3	4	5	6	7	8
Preinversión	$ -								
Inversión Técnica	$ -								
Costos		$ 23.115.000	$ 23.115.000	$ 23.115.000	$ 23.115.000	$ 23.115.000	$ 23.115.000	$ 23.115.000	$ 23.115.000
Gastos		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Acumulado	$ -	$ 23.115.000	$ 46.230.000	$ 69.345.000	$ 92.460.000	$ 115.575.000	$ 138.690.000	$ 161.805.000	$ 184.920.000

Fuente: Autores del texto

Se realiza la diferencia de cada uno de los meses de los dos proyectos para poderlos comparar (Ilustración 32)

Ilustración 32. Diferencia de acumulados de los proyectos

Resultados de Costos de los proyectos									
Periodo	0	1	2	3	4	5	6	7	8
Diferencia de Acumulados	$ 19.098.800	$ 11.470.852	$ 3.842.904	$ (3.785.044)	$ (11.412.992)	$ (19.040.940)	$ (26.668.888)	$ (34.296.836)	$ (41.924.784)

Fuente: Autores del texto

Se observa en la Ilustración 32 el comportamiento de costos de los dos proyectos mutuamente excluyentes, en donde al finalizar se tiene una diferencia entre los dos escenarios de $(41.924.784), teniendo la conclusión que se debe realizar el escenario 1, el cual está generando un ahorro significativo a la compañía.

3. Planeación proyecto

A continuación se relaciona los diferentes ítems requeridos para la correcta implementación del plan de trabajo.

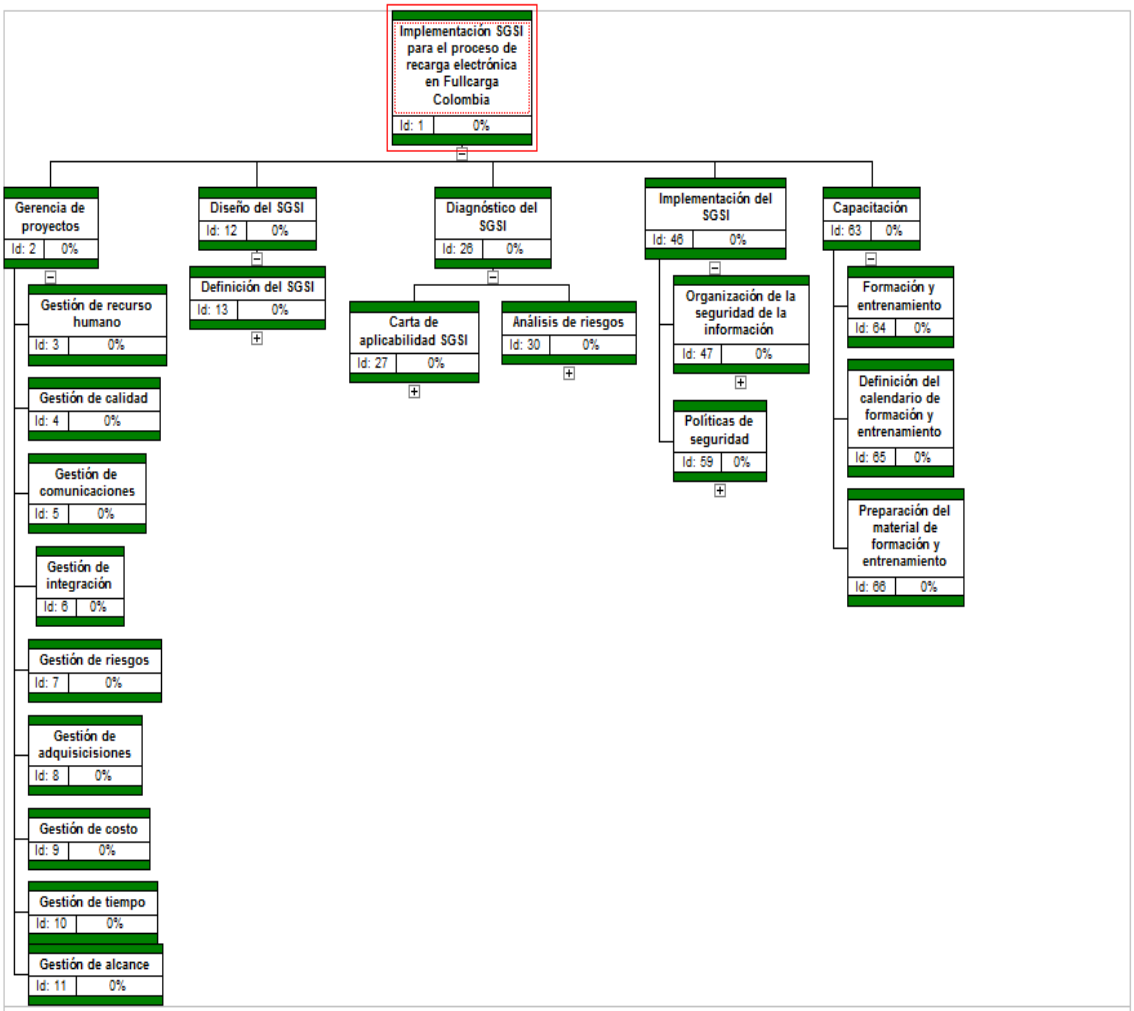
3.1. Alcance – EDT (Estructura de Desglose del Trabajo)

A continuación se podrá observar los entregables del proyecto para poder implementar un SGSI.

3.1.1. EDT tercer nivel

Para mostrar una visual general del proyecto, a continuación se visualizará la EDT de tercer nivel en la Ilustración 33.

Ilustración 33 EDT tercer nivel



Fuente: Autores del trabajo

3.1.1.1. Diccionario de la EDT

A continuación se presentará el diccionario de la EDT (Ilustración 34):

Ilustración 34. Diccionario de la EDT

1.1	**Gerencia del Proyecto**
Descripción	Coordinar, gestionar y controlar bajo las restricciones de alcance, tiempo y recurso, y con un equipo a la altura de las exigencias del proyecto, lo necesario para cumplir con las expectativas de los interesados.
Actividades	- Gestión de recurso humano - Gestión de calidad - Gestión de comunicaciones - Gestión de integración - Gestión de riesgos - Gestión de adquisiciones - Gestión de costo - Gestión de tiempo - Gestión de alcance
Duración	210 días.
Responsable	Equipo del proyecto.
1.2	**Diseño del SGSI**
Descripción	El objetivo de la etapa de Gestión de inicio del SGSI es comprometer a la Dirección, establecer los recursos requeridos, colaboradores y procedimientos a seguir para garantizar la protección, integridad y seguridad de la

	información, identificada en el alcance del SGSI.
Actividades	- Implantación SGSI - Plan de capacitación para la alta gerencia - Gestión para la aprobación del SGSI por la alta gerencia - Publicación de manuales y documentos aprobados - Definición de fundamentos del SGSI - Definir el alcance del SGSI - Definir los objetivos estratégicos de la política de seguridad - Manual de gestión de seguridad de la información - Manual de auditoria de sistemas - Manual de gestión de riesgos - Manual de control de documentos - Manual de mejora continua
Duración	94 días.
Responsable	Equipo del proyecto.
1.3.1	**Diagnóstico del SGSI – carta de aplicabilidad**
Descripción	Para la gestión correcta de la seguridad de la información, se debe identificar, determinar y justificar que controles de la norma ISO 27001; deben ser tomados en cuenta y establecer de manera objetiva las razones específicas de aquellos que no serán tenidos en cuenta.

Actividades	- Aprobación de la de cloración de aplicabilidad - Generar declaración de aplicabilidad
Duración	27 días.
Responsable	Equipo del Proyecto.
1.3.2	**Diagnóstico del SGSI – análisis de riesgos**
Descripción	Se debe establecer la metodología a utilizar para el tratamiento de riesgos, así mismo plantear los procesos afectados y los criterios para la aceptación de riesgos residuales.
Actividades	- Tratamiento de riesgos - Carta de aceptación de riesgos por parte de la alta Gerencia - Plan de tratamiento de riesgos - Aprobación del plan de tratamiento de riesgos - Preparación de los procedimientos para implantar los controles - Selección de los controles de la norma ISO 27002 - Estimación de riesgos - Revisión y confirmación de factores de riesgo - Documento de probabilidad e impacto de factores de riesgo - Estimar y validar tamaño y complejidad de los factores de riesgo - Cálculo del valor de riesgo asociado a cada activo

	- Identificación y evaluación de amenazas y vulnerabilidades de los activos - Identificación de riesgos para cada activo de información - Identificación de los procesos de la cadena de valor de la organización - Inventario de activos de la información
Duración	82 días.
Responsable	Equipo del proyecto.
1.5	**Capacitación - formación general**
Descripción	Se realiza por parte del equipo de trabajo la formación y sensibilización del SGSI; se debe replicar la información entre los empleados sobre los nuevos procedimientos que se van a implantar y concienciar a toda la organización de la importancia que el proyecto de seguridad tiene para la evolución y crecimiento de la empresa.
Actividades	- Formación general - Formación y entrenamiento - Definición del calendario de formación y entrenamiento - Preparación del material de formación y entrenamiento
Duración	57 días.
Responsable	Equipo del proyecto.
1.6	**Implementación**
Descripción	Implementación del plan de tratamiento de riesgos, políticas y procedimientos del SGSI (según corresponda desarrollos y

	cambios adicionales) e implantar los controles seleccionados según se halla definido en la carta de aplicabilidad del SGSI.
Actividades	- Organización de la seguridad de la información - Entrenamiento y entendimiento de los controles - Aprobar y publicar controles y procedimientos - Aplicación de controles - Gestión de las comunicaciones y la operación - Control de acceso - Sistemas de información, adquisición, desarrollo y mantenimiento - Seguridad de la información en la gestión de incidentes - Cumplimiento - Gestión del plan de continuidad de negocio - Seguridad física y ambiental - Seguridad del recurso humano - Políticas de seguridad - Socialización y formación - Aprobación de la política de seguridad - Definición plan de trabajo implementación de los controles
Duración	211 días.
Responsable	Organización - equipo del proyecto.

Fuente: Autores del trabajo

3.1.2. EDT quinto nivel

El EDT de quinto nivel (Ilustración 35), en donde tendremos el grupo final de entregables está relacionado a continuación:

Ilustración 35. EDT quinto nivel

EDT	Nombre de tarea
1	Implementación sistema de gestión de seguridad de la información para el proceso de recarga electrónica en Fullcarga Colombia.
1.1	Gerencia de proyectos.
1.1.1	Gestión de recurso humano.
1.1.2	Gestión de calidad.
1.1.3	Gestión de comunicaciones.
1.1.4	Gestión de integración.
1.1.5	Gestión de riesgos.
1.1.6	Gestión de adquisiciones.
1.1.7	Gestión de costo.
1.1.8	Gestión de tiempo.
1.1.9	Gestión de alcance.
1.2	Diseño del SGSI.
1.2.1	Definición del SGSI.
1.2.1.1	Plan de capacitación para la alta gerencia.
1.2.1.2	Gestión para la aprobación del SGSI por la alta gerencia.
1.2.1.3	Publicación de manuales y documentos aprobados.

EDT	Nombre de tarea
1.2.2	Definición de fundamentos del SGSI.
1.2.2.1	Definir el alcance del SGSI.
1.2.2.2	Definir los objetivos estratégicos de la política de seguridad.
1.2.2.3	Manual de gestión de seguridad de la información.
1.2.2.3.1	Manual de auditoria de sistemas.
1.2.2.3.2	Manual de gestión de riesgos.
1.2.2.3.3	Manual de control de documentos.
1.2.2.3.4	Manual de mejoramiento.
1.3	Diagnóstico del SGCI - carta de aplicabilidad SGSI.
1.3.1	Aprobación de la declaración de aplicabilidad.
1.3.2	Generar "declaración de aplicabilidad".
1.4	Diagnóstico del SGCI - análisis de riesgos.
1.4.1	Tratamiento de riesgos.
1.4.1.1	Carta de aceptación de riesgos por parte de la alta gerencia.
1.4.1.2	Plan de tratamiento de riesgos.
1.4.1.2.1	Aprobación del plan de tratamiento de riesgos.
1.4.1.2.2	Preparación de los procedimientos para implantar los controles.
1.4.1.2.3	Selección de los controles de la norma ISO 27002.
1.4.2	Estimación de riesgos.
1.4.2.1	Revisión y confirmación de factores de riesgo.

EDT	Nombre de tarea
1.4.2.2	Documento de probabilidad e impacto de factores de riesgo.
1.4.2.3	Estimar y validar tamaño y complejidad de los factores de riesgo.
1.4.2.3.1	Cálculo del valor de riesgo asociado a cada activo.
1.4.2.3.2	Identificación y evaluación de amenazas y vulnerabilidades de los activos.
1.4.3	Identificación de riesgos para cada activo de información.
1.4.4	Identificación de los procesos de la cadena de valor de la organización.
1.4.5	Inventario de activos de la información.
1.5	Capacitación.
1.5.1	Formación y entrenamiento.
1.5.2	Definición del calendario de formación y entrenamiento.
1.5.3	Preparación del material de formación y entrenamiento.
1.6	Implementación del SGSI.
1.6.1	Organización de la seguridad de la información.
1.6.1.1	Entrenamiento y entendimiento de los controles.
1.6.1.2	Aprobar y publicar controles y procedimientos.
1.6.1.3	Aplicación de controles.
1.6.1.3.1	Gestión de las comunicaciones y la operación.
1.6.1.3.2	Control de acceso.

EDT	Nombre de tarea
1.6.1.3.3	Sistemas de información, adquisición, desarrollo y mantenimiento.
1.6.1.3.4	Seguridad de la información en la gestión de incidentes.
1.6.1.3.5	Cumplimiento.
1.6.1.3.6	Gestión del plan de continuidad de negocio.
1.6.1.3.7	Seguridad física y ambiental.
1.6.1.3.8	Seguridad del recurso humano.
1.6.2	Políticas de seguridad.
1.6.2.1	Socialización y formación.
1.6.2.2	Aprobación de la política de seguridad.
1.6.2.3	Implementación de los controles.

Fuente: Autores del trabajo

3.2 Programación

A continuación se verá los factores para poder hacer una programación del proyecto efectiva y eficaz, como son las variables de tiempo, costos y riesgos.

3.2.1. Red

El diagrama de red del proyecto se puede observar en el anexo 7 el diagrama de red, donde se puede identificar las actividades e interrelaciones que tiene cada una de ellas y su ruta crítica.

3.2.2. Línea base programación tiempo – alcance

Se observa en el anexo 8 el diagrama de Gantt del proyecto, el cual muestra el cronograma preliminar y su secuencia lógica para poder cumplir el objetivo de implementar un sistema de gestión de seguridad de la información.

3.2.3. Presupuesto – línea base

El presupuesto de la línea base para el proyecto es de COP $108.674.262,44

3.2.4. Indicadores

Los indicadores que se van a usar en el monitoreo y control del proyecto son el de tiempo, presupuesto, socialización del proyecto y nivel de seguridad de la información.

En el indicador de tiempo se va a identificar el porcentaje de avance del proyecto versus el proyectado, el de presupuesto va a calcular el porcentaje ejecutado en costo versus presupuesto, luego se tiene el indicador de socialización que es el porcentaje de quejas y reclamos del proyecto versus la solución de estos.

Por último pero no menos importante el de nivel de seguridad de la información que identifica porcentualmente el avance de los planes de acción frente a la norma ISO 27001:2005, el cual se implementara el autodiagnóstico de la norma, ver Anexo 5. Autodiagnóstico de la ISO 27001 y Anexo 6. Circular 052.

3.2.4.1. Curvas S tiempo y presupuesto

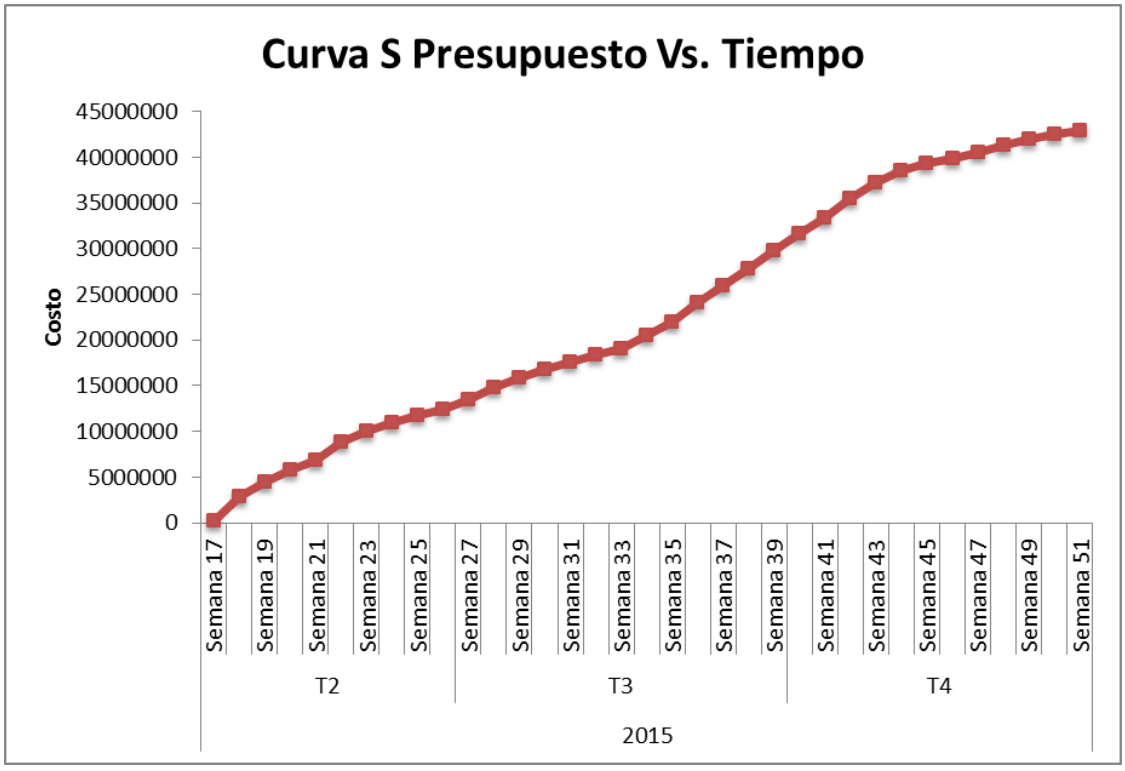
La curva S presupuesto Vs. tiempo permite visualizar el comportamiento de los costos del proyecto presupuestado frente al tiempo e identificar en qué momento se necesita un mayor apalancamiento para tener los recursos, pero como se ve en la

Se puede observar en la Ilustración 36 e Ilustración 37 que las pendientes son muy similares, el motivo de esto es que los costos del proyecto son directamente proporcionales al avance en el tiempo, porque no consta en compra o alquiler de bienes en las tareas sino que están sujetos a los gastos salariales/honorarios de los consultores, que son los responsables de cada una de la ejecución del proyecto.

Ilustración 36 sus costos son lineales y constantes. Igualmente se ve que en la Ilustración 37 el avance del proyecto se ve reflejado lineal.

Se puede observar en la Ilustración 36 e Ilustración 37 que las pendientes son muy similares, el motivo de esto es que los costos del proyecto son directamente proporcionales al avance en el tiempo, porque no consta en compra o alquiler de bienes en las tareas sino que están sujetos a los gastos salariales/honorarios de los consultores, que son los responsables de cada una de la ejecución del proyecto.

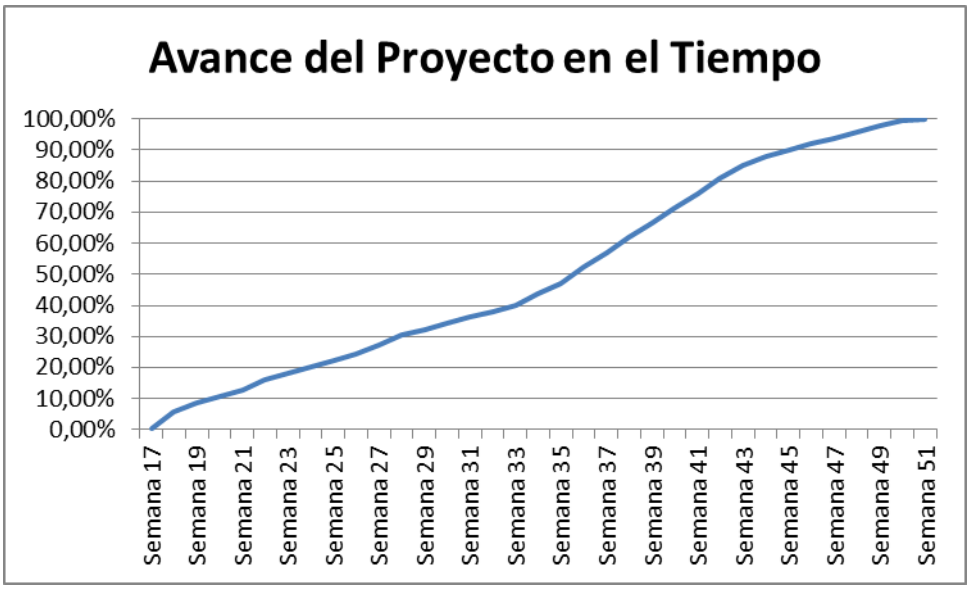
Ilustración 36 Curva S presupuesto Vs. tiempo



Fuente: Autores del texto

Se observa al igual que la ilustración anterior, el avance del proyecto en la Ilustración 37 de manera casi lineal.

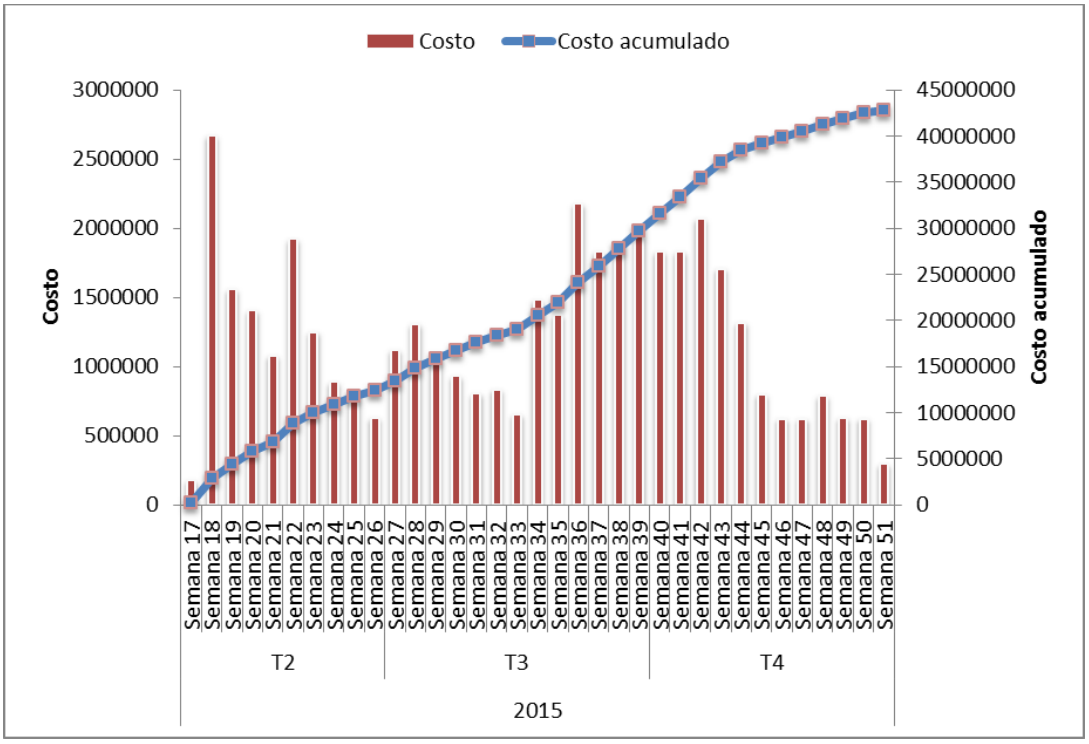
Ilustración 37 Avance del proyecto en el tiempo



Fuente: Autores del texto

A continuación en la Ilustración 38 se relaciona la gráfica de curva S de costo por trimestre

Ilustración 38 Curva S flujo de caja



Fuente: Autores del texto

3.2.5. Riesgos principales

A continuación (Ilustración 39) podemos observar los principales riesgos del desarrollo del proyecto, todos los riesgos del proyecto se pueden detallar en la Ilustración 48

Ilustración 39. Principales riesgos del proyecto

Id.	Descripción del riesgo	Tipo de riesgo	Prob. de ocurrencia	Impacto	Evaluación del riesgo
R07	Pérdida de documentación y/o otros artefactos	Proyecto	40	4	1,6
R09	Inestabilidad del entorno de desarrollo y documentación el proyecto	Proyecto	80	5	4
R10	Mala estimación de costos	Proyecto	50	3	1,5
R11	Falta de seguimiento de tareas	Proyecto	50	3	1,5

Id.	Acciones preventivas	Acciones correctivas
R07	Se usará un repositorio para el control de versiones. Se realizaran copias de seguridad en los ordenadores personales de cada uno de los miembros del equipo de desarrollo.	Actualizar con la última copia disponible.
R09	Asegurar una empresa que brinde garantía de su servicio.	Utilizar una de las computadoras del equipo como servidor.
R10	Realización de varias estimaciones con metodologías diferentes.	Redimensionar el proyecto conforme se ejecuta.
R11	Planificación adecuada de tareas seguimiento del desarrollo de las mismas.	Charla con el equipo de desarrollo en caso de detectarse malas prácticas.

Fuente: Autores del trabajo

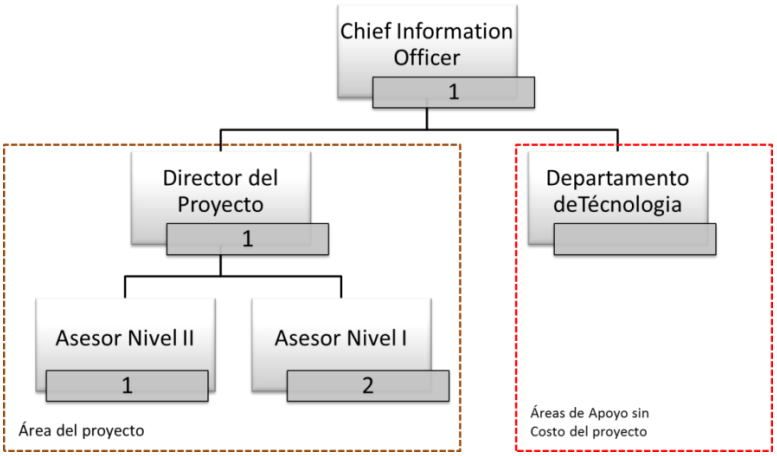
3.2.6. Organización

En esta sección se detallara la estructura organizacional del proyecto y su matriz de responsabilidades a cada una de las personas según el rango que se tenga.

3.2.6.1. Estructura organizacional – OBS-

A continuación se puede observar en la Ilustración 40 el organigrama del proyecto para planear e implementar el SGSI

Ilustración 40. Organigrama del proyecto



Fuente: Autores del texto

.2.6.2. Matriz de responsabilidades – RACI –

A continuación en la Ilustración 41 se podrá observar la matriz de responsabilidades de cada una de las personas que harán parte del proyecto.

Ilustración 41 Matriz RACI

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1	Implementación sistema de gestión de seguridad de la información para el proceso de recarga electrónica en Fullcarga Colombia.				
1.1	Gerencia de proyectos.	A	R		
1.1.1	Gestión de recurso humano.	A	R		
1.1.2	Gestión de calidad.	A	R		
1.1.3	Gestión de comunicaciones.	A	R		
1.1.4	Gestión de integración.	A	R		
1.1.5	Gestión de riesgos.	A	R		
1.1.6	Gestión de adquisiciones.	A	R		
1.1.7	Gestión de costo.	A	R		
1.1.8	Gestión de6 tiempo.	A	R		
1.1.9	Gestión de alcance.	A	R		
1.2	Diseño del SGSI.				
1.2.1	Implantación SGSI				
1.2.1.1	Plan de capacitación para la alta gerencia.	A	R	P	
1.2.1.2	Gestión para la aprobación del SGSI por la alta gerencia.	A	R		

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1.2.1.3	Publicación de manuales y documentos aprobados.		R	R	P
1.2.2	Definición de fundamentos del SGSI.				
1.2.2.1	Definir el alcance del SGSI.	A	R		
1.2.2.2	Definir los objetivos estratégicos de la política de seguridad.	A	R		
1.2.2.3	Manual de gestión de seguridad de la información.				
1.2.2.3.1	Manual de auditoria de sistemas.	V	R	R	P
1.2.2.3.2	Manual de gestión de riesgos.	V	R	R	P
1.2.2.3.3	Manual de control de documentos.	V	R	R	P
1.2.2.3.4	Manual de mejora continua.	V	R	R	P
1.3	Diagnóstico del SGSI - Carta de aplicabilidad SGSI.				
1.3.1	Aprobación de la declaración de aplicabilidad.	A	R	R	P
1.3.2	Generar "declaración de aplicabilidad".	A	R	R	P
1.4	Diagnóstico del SGSI - análisis de riesgos.				
1.4.1	Tratamiento de riesgos.				
1.4.1.1	Carta de aceptación de riesgos por parte de la alta gerencia.	A	R		
1.4.1.2	Plan de tratamiento de riesgos.				
1.4.1.2.1	Aprobación del plan de tratamiento de riesgos.	A	R	P	P
1.4.1.2.2	Preparación de los procedimientos para implantar los controles.		A	R	P
1.4.1.2.3	Selección de los controles de la norma ISO 27002.		A	R	P
1.4.2	Estimación de riesgos.				
1.4.2.1	Revisión y confirmación de factores de riesgo.	A	R	P	P
1.4.2.2	Documento de probabilidad e impacto de factores de riesgo.	A	R	P	P
1.4.2.3	Estimar y validar tamaño y complejidad de los factores de riesgo.				
1.4.2.3.1	Cálculo del valor de riesgo asociado a cada activo.	A	R	v	P
1.4.2.3.2	Identificación y evaluación de amenazas y vulnerabilidades de los activos.	A	R	v	P

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1.4.3	Identificación de riesgos para cada Activo de información.	A	R	v	P
1.4.4	Identificación de los procesos de la cadena de valor de la organización.	A	R	v	P
1.4.5	Inventario de activos de la información.	A	R	v	P
1.5	Capacitación.				
1.5.1	Formación y entrenamiento.	A	R	P	
1.5.2	Definición del calendario de formación y entrenamiento.	A	R	P	
1.5.3	Preparación del material de formación y entrenamiento.	A	R	P	
1.6	Implementación del SGSI.				
1.6.1	Organización de la seguridad de la información.				
1.6.1.1	Entrenamiento y entendimiento de los controles.	A	R	P	
1.6.1.2	Aprobar y publicar controles y procedimientos.	A	R	P	
1.6.1.3	Aplicación de controles.				
1.6.1.3.1	Gestión de las comunicaciones y la operación.	A	R	P	
1.6.1.3.2	Control de acceso.	A	R	P	
1.6.1.3.3	Sistemas de información, adquisición, desarrollo y mantenimiento.	A	R	P	
1.6.1.3.4	Seguridad de la información en la gestión de incidentes.		A	R	P
1.6.1.3.5	Cumplimiento.	A	R	v	p
1.6.1.3.6	Gestión del plan de continuidad de negocio.	A	R	P	
1.6.1.3.7	Seguridad física y ambiental.	A	R	R	P
1.6.1.3.8	Seguridad del recurso humano.	A	R	R	P
1.6.2	Políticas de seguridad.				
1.6.2.1	Socialización y formación.	A	R	R	P
1.6.2.2	Aprobación de la política de seguridad.	A	R	R	P
1.6.2.3	Implementación de los controles.	A	R	R	P

Códigos de Responsabilidad		Código de Roles	
A	Aprueba el entregable	PA	Patrocinador
R	Responsible del entregable	GP	Gerente del Proyecto
P	Participa	AS II	Asesor Nivel II
V	Revisa	AS I	Asesor Nivel I

Fuente: Autores del texto

3.3 Planes de gestión

A continuación se podrá observar los planes de gestión para el proyecto “Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.”.

PLAN DE GESTIÓN DE LA INTEGRACIÓN DEL PROYECTO

En este plan se busca definir, identificar, unificar y coordinar todos los procesos y actividades del proyecto desde la etapa de inicio hasta la etapa de cierre.

El plan de gestión del proyecto “Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.”, consta de:

- Plan de gestión de la integración del proyecto.
- Plan de gestión de control de cambios.
- Plan de gestión del alcance del proyecto.
- Plan de gestión del tiempo del proyecto.
- Plan de gestión de los costos del proyecto.
- Plan de gestión de la calidad del proyecto.
- Plan de gestión de los recursos humanos del proyecto.
- Plan de gestión de las comunicaciones del proyecto.
- Plan de gestión de los riesgos del proyecto.
- Plan de gestión de las adquisiciones del proyecto.

PLAN DE GESTIÓN DE ALCANCE[1]

La definición del alcance del proyecto de aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia, se desarrollará en reunión de equipo de proyecto, en donde junto con el *sponsor* se revisará el *Scope Statement* preliminar, el cual servirá como base.

Los requerimientos necesarios para la definición del sistema de gestión de calidad de la información de la organización Fullcarga Colombia, será por medio de entrevistas cerradas a los interesados y se documentará utilizando UML (*Unified Modeling Language*), lenguaje de modelado de sistemas; aunque principalmente utilizado para el desarrollo de software, logra visualizar, especificar, construir y documentar de forma clara un sistema y será una fuente documental clave para la mejora de los procesos.

Proceso para la elaboración de EDT:

Para la elaboración de la EDT se realizaron los siguientes pasos:

- El EDT del proyecto será estructurado identificándose los principales entregables, que en el proyecto actúan como fases, en el proyecto se identificó un total de 3 fases: diagnóstico, puesta en producción (implantación y operación) y gerencia de proyectos.
- Identificado los principales entregables, se procede con la descomposición del entregable en paquetes de trabajo, los cuales nos permitirán conocer al mínimo el detalle el costo, trabajo y calidad incurrida en la elaboración del entregable.
- Se utilizará la herramienta *WBS Chart Pro* para la diagramación de la EDT.

Proceso para la elaboración del diccionario de EDT:

Es con base a la información del EDT se elaborará el diccionario, para lo cual se realizarán los siguientes pasos:

[1] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: http://dharmacon.net/site/

- Elaboración de plantilla diseñada para dicho fin.
- Se identifica las siguientes características de cada paquete de trabajo del EDT.
    - Se detalla el objetivo del paquete de trabajo.
    - Se hace una descripción breve del paquete de trabajo.
    - Se describe el trabajo a realizar para la elaboración del entregable, como son la lógica o enfoque de elaboración y las actividades para elaborar cada entregable.
    - Se establece la asignación de responsabilidad, donde por cada paquete de trabajo se detalla quién hace qué: responsable, participa, apoya, revisa, aprueba y da información del paquete de trabajo.
    - De ser posible se establece las posibles fechas de inicio y fin del paquete de trabajo, o un hito importante.
    - Se describe cuáles son los criterios de aceptación.

Proceso para verificación de alcance:

Al término de elaboración de cada entregable, éste debe ser presentado al Sponsor del Proyecto, el cual se encargará de aprobar o presentar las observaciones del caso. Si el entregable es aprobado, será entregado al comité primario de la compañía.

Proceso para control de alcance:

En este caso se presentan dos variaciones:

Primero, el *Project Manager* se encarga de verificar que el entregable cumpla con lo acordado en la línea Base del Alcance. Si el entregable es aprobado, es enviado al comité primario de la organización. De lo contrario, el entregable es devuelto a su responsable junto con una Hoja de Correcciones, donde se señala cuáles son las correcciones o mejoras que se deben hacer

Segundo, se puede presentar sus observaciones respecto al entregable, para lo cual requerirá reunirse con el *Project Manager*, y presentar sus requerimientos de cambio o ajuste.

PLAN DE GESTIÓN DE TIEMPO[2]

A continuación se puede observar los procesos definidos para el plan de gestión de tiempo:

Proceso de definición de actividades:

Partiendo de la revisión de cada actividad y el orden de las precedencias de actividades, teniendo presente cada punto a continuación descrito:

- Por cada entregable definido en el EDT del proyecto se identifica cuáles son las actividades que permitirán el término del entregable.
- Para tal caso se da un código, nombre y alcance de trabajo, zona geográfica, responsable y tipo de actividad, para cada actividad del entregable.
- Inicialmente definimos el orden de secuencia de las actividades por cada entregable.

Proceso de orden de secuencia de actividades:

- Definir la red de proyectos.
- Luego por separado graficamos la red del proyecto de las actividades de cada fase del proyecto.
- Se identifican las tareas críticas y se definen los tiempos de holgura a manejar.

Proceso de estimación de recursos:

- Basados en los entregables y actividades que se han identificado para el proyecto se procede a realizar las estimaciones de la duración y el tipo de recursos (personal, materiales o consumibles).
- Para el Recurso de tipo Personal se define los siguientes datos: nombre de recurso, trabajo, duración, supuestos y base de estimación, y forma de cálculo.

[2] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: ***http://dharmacon.net/site/***

- Para el recurso de tipo Materiales o Consumibles se define los siguientes: nombre de recurso, cantidad, supuestos y base de estimación, y forma de cálculo.
- Para este proceso utilizamos el formato de estimación de Recursos y Duraciones.
- El proceso de estimación del tiempo de las actividades se define de acuerdo al tipo de recurso asignado a la actividad, si el recurso es tipo personal, estimamos la duración y calculamos el trabajo que tomará realizarla.

Proceso de estimación de recursos de las actividades

Para la definición de los recursos de las actividades se tomará cada entregable y se procederá a realizar las estimaciones de la duración y el recurso (personal, materiales o consumibles, y no consumibles).

Para el recurso de tipo personal se define los siguientes:

- Nombre de recurso,
- Trabajo,
- Duración,
- Supuestos,
- Base de estimación, y forma de cálculo.

Para el recurso de tipo material o consumible se define los siguientes:

- Nombre de recurso,
- Cantidad,
- Supuestos,
- Base de estimación, y forma de cálculo.

Para el recurso de tipo máquinas o no consumibles se define los siguientes:

- Nombre de recurso,
- Cantidad,
- Supuestos,

- Base de estimación, y forma de cálculo

Para este proceso utilizamos el formato de estimación de recursos y duraciones definido por el equipo del proyecto.

Proceso de estimación de duración de las actividades:

El proceso de estimación de la duración de las actividades se define de acuerdo al tipo de recurso asignado a la actividad:

- Si el recurso es tipo personal, estimamos la duración y calculamos el trabajo que tomará realizar la actividad.
- Si el tipo de recurso es material o máquinas, se define la cantidad que se utilizará para realizar la actividad.

Proceso de desarrollo del cronograma:

En base a los siguientes documentos:

- Identificación y creación de la secuencia de actividades.
- Red del proyecto.
- Estimación de recursos y duraciones.

Con toda la información necesaria para elaborar el cronograma del proyecto, mediante la herramienta de *MS Project 2010*, realizando los siguientes pasos:

Paso 1: Crear un proyecto: se crea un nuevo plan de proyecto en blanco.

Paso 2: Agregar tareas al proyecto, se toma la lista de tareas cuya complejidad irá aumentando hasta convertirse, en un plan y una programación completamente desarrollados. Una vez que haya creado o importado su lista tareas, podrá definir la relación entre las mismas.

Crear los hitos o tareas que sirven de punto de referencia y marcan los eventos principales del proyecto.

Establecer la duración de una tarea, determinar en cuánto tiempo se completará una tarea y agregar esta información al plan para finalizar este paso efectué la vinculación (dependencias) entre las tareas de la lista de tareas.

Paso 3: Organizar la lista de tareas y hacer que sea más clara de leer con tan solo aplicar sangrías a las tareas del proyecto para crear así un esquema de las tareas de resumen y las subtareas a imagen de la EDT establecida.

Paso 4: Crear los calendarios de trabajo y ajustar la programación. Se debe establecer calendarios para todo el proyecto, para tareas específicas y para recursos que trabajen en el proyecto.

Paso 5: Damos propiedades a las actividades y asignamos los recursos de las actividades del proyecto.

Paso 6: Guardar y enviar para aprobación al patrocinador, se debe guardar el proyecto periódicamente para mantener los cambios realizados. Hacer una copia de seguridad y mantener en un lugar independiente al de trabajo. El cronograma es enviado al *sponsor*, el cual debe aprobar el documento para proseguir con el proyecto.

Proceso de control del cronograma:

Dentro de la gestión del proyecto, se usara el entregable del informe de rendimiento del trabajo e Informe de rendimiento del proyecto, y se tendrá como evidencia de control, las reuniones de coordinación. Ante la aprobación de una solicitud de cambio presentada por el comité de control de cambios, se hacen las modificaciones aprobadas o si fuera el caso se hace nuevamente la planificación del proyecto.

Sistema de control de tiempos:

Cada responsable del equipo de proyecto emite un reporte semanal informando los entregables realizados y el porcentaje de avance.

El gerente de proyecto se encarga de compactar la información del equipo de proyecto en el cronograma de trabajo, actualizando el proyecto según los

reportes del equipo, y procede a re planificar el proyecto en el escenario del MS PROJECT 2010. De esta manera se actualiza el estado del proyecto, y se emite el informe semanal del rendimiento del proyecto.

La duración del proyecto puede tener una variación de +/- 10 % del total planeado, si estos márgenes son superados se necesitará emitir una solicitud de cambio, la cual deberá ser revisada y aprobada por el gerente de proyecto y el Sponsor.

El avance será medido utilizando la metodología de la gestión ágil de proyectos (*Scrum*) la cual tiene como objetivo dar evidencia a las demandas principales de la organización: valor, reducción del tiempo de implementaciones, agilidad, flexibilidad y fiabilidad, permitiendo evidencia retrasos futuros y tomando acciones correctivas a tiempo; siempre soportados sobre los reportes de avance mensuales, que deben incluir análisis del progreso de las actividades y el recurso utilizado.

PLAN DE GESTIÓN DE COSTO[3]

A continuación se observara el plan de gestión de costo del proyecto.

Tipos de estimación del proyecto:

Tipo de estimación	Formulación	Nivel de precisión
Orden de magnitud	Formulación por comparación con proyectos similares	- 25% al +75%
Presupuesto	Cotizaciones y experiencia del equipo de trabajo	- 15% al +25%
Definitivo	Cotizaciones y experiencia del equipo de trabajo	- 5% al +10%
Reserva de contingencia	Experiencia del equipo de trabajo y conocimiento de expertos	- 5% al +10%
Reserva administrativa	Se tomará sobre el presupuesto definitivo establecido y corresponderá al 5% de este valor.	-1% al +3%

Unidades de medida:

Tipo de recurso	Unidad de medida
Recurso personal	Costo hora hombre
Recurso material o consumible	Unidades
Recurso máquina o no consumible	Unidades

[3] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: ***http://dharmacon.net/site/***

Planificación:

La forma y definición en que se utilizará la planificación del dinero definiendo las etapas y los niveles de agregación de los componentes de planificación, así como la fecha en que se emitirán los presupuestos no expandidos estará a cargo del ingeniero Daniel Gutiérrez como líder financiero del proyecto, soportado por el gerente financiero de Fullcarga Colombia.

Se define el presupuesto a partir de las necesidades de la organización y se ajusta a la restricción establecida por la organización del presupuesto asignado del departamento de tecnología para el desarrollo del proyecto.

Alcance: proyecto / fase / entregable: Proyecto completo.

Variación permitida: +/- 5% costo planificado.

Acción a tomar si la variación excede lo permitido: Se debe Investigar variación para tomar acción correctiva y en caso de presentar sobrecostos, debe ser aprobado por el comité primario de la empresa.

Tipo de pronóstico: EAC variaciones atípicas

Formula: AC + (BAC-EV)/CPI

Control: Informe de rendimiento del proyecto presentado semanalmente.

Niveles de estimación: se establece un orden de magnitud por fase y presupuesto por actividad

Procesos de gestión de costos: se puede ver a continuación los procesos de gestión de costos para el proyecto.

Proceso de gestión de costos	Descripción
Estimación de costos	Se estima los costos del proyecto con base al tipo de estimación por presupuesto y definitiva. Esto se realiza en la planificación del proyecto y es responsabilidad del gerente de proyecto, y aprobado por el Sponsor.
Preparación del presupuesto de costos	Se elabora el presupuesto del proyecto y las reservas de gestión del proyecto. Este documento es elaborado por el gerente del proyecto, revisado y aprobado por el Sponsor.
Control de costos	Se evaluará el impacto de cualquier posible cambio del costo, informando al Sponsor los efectos en el proyecto, en especial las consecuencias en los objetivos finales del proyecto (alcance, tiempo y costo). El análisis de impacto deberá ser presentado al Sponsor y evaluará distintos escenarios posibles, cada uno de los cuales corresponde a alternativas de intercambio de triple restricción. Toda variación final dentro del +/- 5% del presupuesto será considerada como normal. Toda variación final fuera del +/- 5% del presupuesto será considerada como causa asignable y deberá ser auditada. Se presentará un informe de auditoría, y de ser el caso se generará una lección aprendida.

Fuente: autores del trabajo

Plan de gestión de costos: documento que informa la planificación para la gestión del costo del proyecto.

Línea base del costo: línea base del costo del proyecto, sin incluir las reservas de contingencia

Costeo del proyecto: este informe detalla los costos a nivel de las actividades de cada entregable, según el tipo de recurso que participe.

Presupuesto por fase y entregable: informa los costos del proyecto, divididos por fases, y cada fase dividido en entregables.

Presupuesto por fase y por tipo de Recurso: informe de los costos del proyecto divididos por fases, y cada fase en los 3 tipos de recursos (personal, materiales o maquinaria).

Presupuesto en el tiempo (Curva S): la curva S muestra la gráfica del valor ganado del proyecto en un periodo de tiempo.

Sistema de control de cambios de costos:

El *sponsor* y el gerente de proyecto son los responsables de evaluar, aprobar o rechazar las propuestas de cambios.

Se aprobarán automáticamente aquellos cambios de emergencia que potencialmente puedan impedir la normal ejecución del proyecto, y que por su naturaleza no puedan esperar a la reunión del Comité primario, y que en total no excedan del 5% del presupuesto aprobado del proyecto.

Estos cambios deberán ser expuestos en la siguiente reunión del equipo del proyecto. Todos los cambios de costos deberán ser evaluados integralmente, teniendo en cuenta para ello los objetivos del proyecto y los intercambios de la triple restricción.

Los documentos que serán afectados o utilizados en el control de cambios de costos son:

- Solicitud de Cambios.

- Acta de reunión de coordinación del proyecto.
- Plan del Proyecto (volver a planificación de todos los planes que sean afectados)

En primera instancia el que tiene la potestad de resolver cualquier disputa relativa al tema es el gerente de proyecto, si está no puede ser resuelta por él, es el Sponsor que asume la responsabilidad.

Una solicitud de cambio sobre el coste del proyecto que no exceda el +/- 5% del presupuesto del proyecto puede ser aprobada por el gerente del proyecto, un requerimiento de cambio superior será resuelta por el Sponsor.

PLAN DE GESTIÓN DE LA CALIDAD[4]

A continuación se relaciona los ítems del plan de Gestión de Calidad del proyecto:

Políticas de calidad del proyecto:

Este proyecto debe cumplirse con los requisitos de calidad implementados en FullCarga Colombia, realizándolo en el tiempo y costos establecidos.

Línea base de calidad del proyecto:

Los indicadores para definir la línea base de calidad del proyecto se definieron en cuatro: 1. Costo 2. Tiempo 3. Socialización 4. Nivel de Seguridad de la Información, los cuales se puede observar a continuación en la Ilustración 42.

Ilustración 42. Métricas del proyecto

Nombre	**Indicador**	
Costo	Descripción	Porcentaje de utilización de presupuesto del proyecto
	Frecuencia	Quincenal
	Cálculo	$\frac{Costo\ Real}{Presupuesto}$
	Meta	Entre 90% y 100%
Tiempo	Descripción	Porcentaje de avance del proyecto referente al cronograma
	Frecuencia	Quincenal
	Cálculo	$\frac{Ejecutado}{Programado}$
	Meta	Entre 95% y 105%
Socialización	Descripción	Porcentaje de Problemas, Quejas y reclamos presentados en el proyecto versus la solución de estos.
	Frecuencia	Quincenal
	Cálculo	$\frac{\#PQR\ Solucionadas}{\#PQR\ Presentada}$
	Meta	Mínimo 80%
Nivel de seguridad de la información	Descripción	Identificación porcentual del avance de los planes de acción de control de seguridad frente la norma ISO 27001:2005
	Frecuencia	Quincenal
	Cálculo	$\frac{\#\ de\ Control\ con\ plan\ de\ acción}{\#\ de\ controles\ de\ la\ norma\ ISO\ 27001}$
	Meta	Mínimo 90%

Fuente: Autores del texto

[4] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: ***http://dharmacon.net/site/***

Matriz de actividades de calidad:

A continuación en la Ilustración 43 se identifica los estándares aplicables según el entregable:

Ilustración 43. Matriz de estándares aplicables

No. WBS	Paquete de trabajo	Estándar o Norma de calidad aplicable	Actividades de prevención	Actividades de control
1.1.1.1	Plan de capacitación para la alta gerencia	Metodología GP de Fullcarga		Aprobación por esponsor
1.1.1.2	Gestión para la aprobación del SGSI por la Alta Gerencia	Metodología GP de Fullcarga	Revisión detallada	Aprobación por esponsor
1.1.1.3	Publicación de manuales y documentos aprobados	Metodología GP de Fullcarga		Revisión por el Gerente del proyecto
1.1.2.1	Definir el alcance del SGSI	Metodología GP de Fullcarga		Aprobación por esponsor
1.1.2.2	Definir los objetivos estratégicos de la Política de Seguridad	Metodología GP de Fullcarga		Aprobación por esponsor
1.1.2.3.1	Manual de auditoria de sistemas	Formato exigido por el Proyecto	Revisión de modelos de formatos	Revisión por el Gerente del proyecto
1.1.2.3.2	Manual de Gestión de Riesgos	Formato exigido por el Proyecto	Revisión de modelos de formatos	Revisión por el Gerente del proyecto
1.1.2.3.3	Manual de control de documentos	Formato exigido por el Proyecto	Revisión de modelos de formatos	Revisión por el Gerente del proyecto
1.1.2.3.4	Manual de mejora continua	Formato exigido por el Proyecto	Revisión de modelos de formatos	Revisión por el Gerente del proyecto
1.2.1	Aprobación de la declaración de aplicabilidad	Metodología GP de Fullcarga		Aprobación por esponsor
1.2.2	Generar "Declaración de Aplicabilidad"	Metodología GP de Fullcarga		Aprobación por esponsor
1.3.1.1	Carta de aceptación de riesgos por parte de la alta Gerencia	Formato exigido por el Proyecto	Revisión de modelos de formatos	Aprobación por esponsor
1.3.1.2.1	Aprobación del plan de tratamiento de riesgos	Metodología GP de Fullcarga		Aprobación por esponsor
1.3.1.2.2	Preparación de los procedimientos para implantar los controles	Metodología GP de Fullcarga		Revisión por el Gerente del proyecto
1.3.1.2.3	Selección de los controles de la norma ISO 27002	ISO 27002	Revisión detallada	Revisión por el Gerente del proyecto
1.3.2.1	Revisión y confirmación de factores de riesgo	ISO 27005		Revisión por el Gerente del proyecto
1.3.2.2	Documento de probabilidad e impacto de factores de riesgo	ISO 27005		Revisión por el Gerente del proyecto
1.3.2.3.1	Cálculo del valor de riesgo asociado a cada activo	ISO 27005	Revisión detallada	Revisión por el Gerente del proyecto
1.3.2.3.2	Identificación y evaluación de amenazas y vulnerabilidades de los activos	ISO 27005	Revisión detallada	Revisión por el Gerente del proyecto
1.3.3	Identificación de Riesgos para cada Activo de información	ISO 27005		Revisión por el Gerente del proyecto
1.3.4	Identificación de los procesos de la cadena de valor de la organización	Metodología GP de Fullcarga	Revisión de estándar	Revisión por el Gerente del proyecto
1.3.5	Inventario de activos de la información		Revisión detallada	Aprobación por esponsor
1.4	Formación y sensibilización	Metodología Fullcarga Colombia		Aprobación por esponsor
1.5	Preparación certificación	ISO/IEC 27001:2005	Revisión de estándar	Aprobación por esponsor
1.6	Gerencia de Proyectos	PMBOK		Aprobación por esponsor

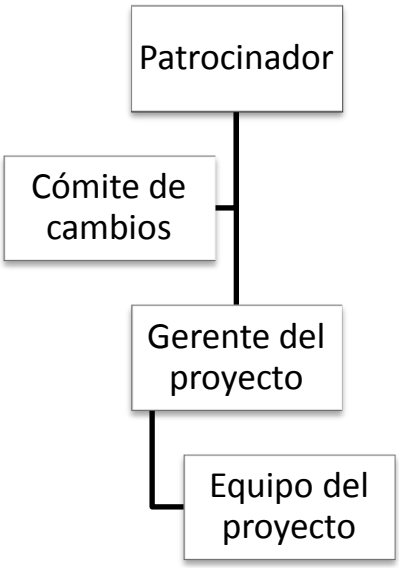
Fuente: Autores del texto

Roles para la gestión de la calidad:

PATROCINADOR	**Objetivos del rol:**
	Responsable ejecutivo y final por la calidad del proyecto
	Funciones del rol:
	Revisar, aprobar y tomar acciones correctivas para mejorar la calidad
	Niveles de autoridad:
	Aplicar a discreción de Fullcarga Colombia los recursos para el proyecto.
	Reporta a:
	Junta directiva
	Supervisa a:
	Gerente de proyecto
	Requisitos de conocimiento:
	Gerencia de Proyectos y Gestión en general
	Requisitos de Habilidades:
	Liderazgo, comunicación, negociación, motivación y solución de conflictos
GERENTE DEL PROYECTO	**Objetivos del rol:**
	Gestionar operativamente la calidad
	Funciones del rol:
	Revisar estándares, revisar entregables, aceptar entregables o disponer su reproceso, deliberar para generar acciones correctivas, aplicar acciones correctivas
	Niveles de autoridad:
	Exigir cumplimiento de los entregables al equipo del proyecto
	Reporta a:
	Patrocinador
	Supervisa a:
	Equipo del proyecto
	Requisitos de conocimiento:
	Gerencia de Proyectos
	Requisitos de Habilidades:
	Liderazgo, comunicación, negociación, motivación y solución de conflictos
EQUIPO DE PROYECTO	**Objetivos del rol:**
	Elaborar los entregables con la calidad y estándares requeridos
	Funciones del rol:
	Elaborar los entregables
	Reporta a:
	Gerente del proyecto
	Supervisa a:
	NA
	Requisitos de conocimiento:
	Especifica según los entregables
	Requisitos de habilidades:
	Especifica según los entregables

Fuente: Autores del texto

Organización para la calidad del proyecto:



Fuente: Autores del texto

Documentos normativos para la calidad:

Procedimientos	1. Mejora de procesos
	2. Auditoria de procesos
	3. Reuniones de aseguramiento de la calidad
	4. Resolución de problemas
Plantillas	1. Métricas
	2. Plan de gestión de la calidad
Formatos	1. Métricas
	2. Línea base de la calidad
	3. Plan de gestión de la calidad
Listas de chequeo	1. De métricas
	2. De auditorias
	3. Acciones correctivas

Fuente: autores del trabajo

Procesos de gestión de la calidad

A continuación se enumeraran los procesos de gestión de calidad:

1. **Enfoque de aseguramiento de la calidad**

   El aseguramiento de calidad se hará monitoreando continuamente el rendimiento del trabajo, los resultados del control de calidad y sobre todo las métricas. De esta manera se descubrirá tempranamente cualquier necesidad de auditoria de procesos o de mejora. Los resultados se formalizarán como solicitudes de cambio o acciones correctivas/ preventivas. Asimismo se verificará que dichas solicitudes se hayan ejecutado y siendo efectivas.

2. **Enfoque de control de la calidad**

   El control de calidad se ejecutará revisando los entregables del proyecto para ver si están a conformidad o no. Los resultados de estas mediciones se consolidarán y se enviaran al proceso de aseguramiento de calidad.

   Asimismo en este proceso se hará la medición de las métricas y se informará al proceso de aseguramiento de la calidad. Los entregables que han sido reprocesados se volverán a revisar para verificar si ya se han vuelto conformes. Para los defectos detectados se tratará de identificar las causas principales del problema para eliminar las fuentes del error, los resultados y conclusiones se formalizarán como solicitudes de cambio y/o acciones correctivas/preventivas.

3. **Enfoque de mejora de procesos**

   Cada vez que se deba mejorar un proceso se seguirán los siguientes pasos:

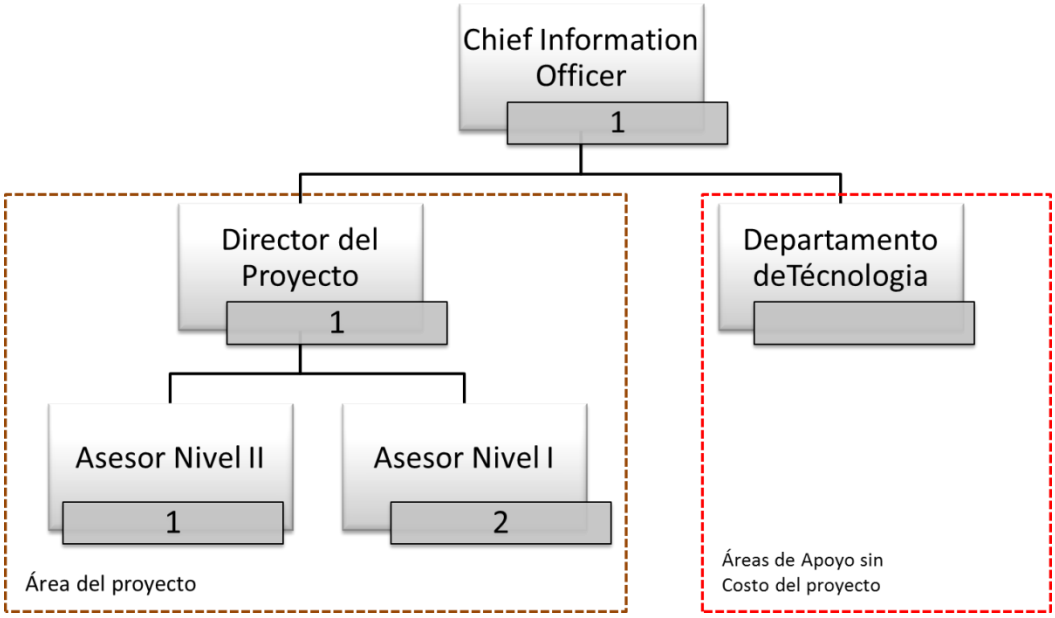
   1. Delimitar el proceso
   2. Determinar la oportunidad de mejora
   3. Tomar información sobre el proceso

4. Analizar la información levantada
5. Definir las acciones correctivas para mejorar el proceso
6. Aplicar las acciones correctivas
7. Verificar si las acciones correctivas han sido efectivas
8. Estandarizar las mejoras logradas para hacerlas parte del proceso

PLAN DE GESTIÓN DE RECURSOS HUMANOS[5]

A continuación se relaciona los ítems del plan de gestión de recursos humanos del proyecto:

Organigrama del proyecto:



Fuente: Autores del texto

Roles y responsabilidades:

A continuación se relacionan los roles del proyecto.

Nombre del Rol
Patrocinador (*Chief Information Officer*)
Objetivos del rol
Es la persona que patrocina el proyecto, es el principal interesado en el éxito del proyecto, y por tanto la persona que apoya, soporta, y defiende el proyecto.
Responsabilidades

[5] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: ***http://dharmacon.net/site/***

1. Aprobar el *Project Charter*. 2. Aprobar el *Scope Statement.* 3. Aprobar el plan de proyecto. 4. Aprobar el cierre del proyecto. 5. Aprobar todos los informes de avance del proyecto. 6. Revisar el informe final.
Funciones
Las funciones del patrocinador son: 1. Iniciar el proyecto. 2. Aprobar la planificación del proyecto. 3. Monitorear el estado general del proyecto. 4. Cerrar el proyecto y el contrato de servicio. 5. Gestión ar el control de cambios. 6. Asignar recursos al proyecto. 7. Designar y empoderar al Director del proyecto. 8. Ayudar en la solución de problemas y superación de obstáculos del proyecto.
Niveles de Autoridad
Decide sobre recursos humanos y materiales asignados al proyecto, decide sobre modificaciones a las líneas base del proyecto. Decide sobre planes y programas del proyecto.
Reporta A:
Supervisa A:
Gerente del proyecto

Fuente: Autores del texto

Nombre del Rol
Gerente del proyecto
Objetivos del rol
Es la persona que gestionará el proyecto, es el principal responsable por el éxito del proyecto, y por tanto la persona que asume el liderazgo y la administración de los recursos del proyecto para lograr los objetivos fijados por

el Sponsor.	
Responsabilidades	
1. Elaborar el *Project Charter*. 2. Elaborar el *Scope Statement*. 3. Elaborar el Plan de Proyecto. 4. Elaborar el Informe de Estado del Proyecto. 5. Realizar la Reunión de Coordinación Semanal. 6. Elaborar el Informe de Cierre del proyecto. 7. Elaborar el Informe con los planes de acción definidos.	
Funciones	
Las funciones del Gerente de proyecto son: 1. Ayudar al Sponsor a iniciar el proyecto. Planificar el proyecto. 2. Ejecutar el proyecto. Controlar el proyecto. 3. Cerrar el proyecto. 4. Ayudar a Gestión ar el Control de Cambios del proyecto. 5. Ayudar a Gestión ar los temas contractuales con el Cliente. 6. Gestión ar los recursos del proyecto.7. Solucionar problemas y superar los obstáculos del proyecto	
Niveles de Autoridad	
Decide sobre la programación detallada de los recursos humanos y materiales asignados al proyecto. Decide sobre la información y los entregables del proyecto. Decide sobre los proveedores y contratos del proyecto, siempre y cuando no excedan lo presupuestado.	
Reporta A:	
Patrocinador	
Supervisa A:	
Asesores nivel I y II	
Requisitos del Rol:	
Conocimientos	• Gestión de proyectos según la guía *PMBOK*®. • MS Project. • Estándares de aseguramiento de la información (ISO 27001, Cobit 4, ITL)
Habilidades	Liderazgo, comunicación, negociación, solución de conflictos y motivación.
Experiencia	• Gestión de proyectos según la guía *PMBOK*® (2 años). • *MS Project* (2 años). • Estándares de aseguramiento de la información

	(ISO 27001, Cobit 4, ITL) (5 años)

Fuente: Autores del texto

Nombre del Rol
Asesor nivel II
Objetivos del rol
Apoyar en la ejecución del proyecto y revisar los planes de acción de los controles de aseguramiento de la información.
Responsabilidades
1. Participa en la elaboración de los planes de acción de los controles de seguridad. 2. Participa en las reuniones de avance del proyecto. 3. Participa en el levantamiento de información de la compañía.
Funciones
1. Revisar el levantamiento de información y verificarlo. 2. Revisar los planes de acción de controles de seguridad de la información. 3. Vigilar el desarrollo de las actividades. 4. Revisar las respuestas y planes de acción a las quejas y reclamos del proyecto.
Niveles de Autoridad
Decide sobre los planes de acción para los controles de aseguramiento de la información basados en la ISO 27001.
Reporta A:
Gerente del proyecto

Supervisa A:	
Requisitos del Rol:	
Conocimientos	• Gestión de proyectos según la guía *PMBOK*®. • MS Project. • Estándares de aseguramiento de la información (ISO 27001, Cobit 4, ITL)
Habilidades	Liderazgo, comunicación, negociación, solución de conflictos y motivación.
Experiencia	• Gestión de proyectos según la guía *PMBOK*® (1 años). • MS Project (1 años). • Estándares de aseguramiento de la información (ISO 27001, Cobit 4, ITL) (2 años)

Fuente: Autores del texto

Nombre del Rol
Asesor nivel I
Objetivos del rol
Apoyar en la ejecución del proyecto y elaborar los planes de acción de los controles de aseguramiento de la información

Responsabilidades	
1. Participa en la elaboración de los planes de acción de los controles de seguridad. 2. Participa en las reuniones de avance del proyecto. 3. Participa en el levantamiento de información de la compañía.	
Funciones	
1. Elaborar el levantamiento de información y verificarlo. 2. Elaborar los planes de acción de controles de seguridad de la información.	
Niveles de Autoridad	
Reporta A:	
Gerente del proyecto	
Supervisa A:	
Requisitos del Rol:	
Conocimientos	Gestión de proyectos según la guía PMBOK®. MS Project. Estándares de aseguramiento de la información (ISO 27001, Cobit 4, ITL)
Habilidades	Liderazgo, comunicación, negociación, solución de conflictos y motivación.
Experiencia	Gestión de proyectos según la guía *PMBOK*® (1 año).

	MS Project (1 año). Estándares de aseguramiento de la información (ISO 27001, Cobit 4, ITL) (1 año)

Fuente: Autores del texto

Adquisición del personal del proyecto:

A continuación se puede observar la prioridad y tiempo de adquisición de las personas del proyecto.

No.	Rol	Tipo de adquisición	Fuente de adquisición	Modalidad de adquisición
1	Patrocinador	Pre asignación	Fullcarga Colombia S.A.	
2	Director del proyecto	Pre asignación	Fullcarga Colombia S.A.	Decisión del patrocinador
3	Asesor nivel II	Contratación	Elempleo.com	Contratación directa
4	Asesor nivel I	Contratación	Elempleo.com	Contratación directa
No.	**Fecha de inicio de reclutamiento**	**Fecha requerida de disponibilidad**	**Costo de reclutamiento**	**Apoyo área de RRHH**
1		01/02/2013	Ninguno	Ninguno
2		01/02/2013	Ninguno	Ninguno
3	15/01/2013	01/02/2013	Ninguno	Ninguno
4	15/01/2013	01/02/2013	Ninguno	Ninguno

Fuente: Autores del texto

Matriz raci

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1	Implementación sistema de gestión de Seguridad de la Información para el proceso de recarga electrónica en Fullcarga Colombia.	A	R	I	I
1.1	Gerencia de proyectos.	A	R	I	I
1.1.1	Gestión de recurso humano.	A	R	I	I
1.1.2	Gestión de calidad.	A	R	I	I
1.1.3	Gestión de comunicaciones.	A	R	I	I
1.1.4	Gestión de integración.	A	R	I	I
1.1.5	Gestión de riesgos.	A	R	I	I
1.1.6	Gestión de adquisiciones.	A	R	I	I
1.1.7	Gestión de costo.	A	R	I	I
1.1.8	Gestión de tiempo.	A	R	I	I
1.1.9	Gestión de alcance.	A	R	I	I
1.2	Diseño del SGSI.				
1.2.1	Definición del SGSI.				
1.2.1.1	Plan de capacitación para la alta gerencia.	A	R	P	
1.2.1.2	Gestión para la aprobación del SGSI por la alta gerencia.	A	R		
1.2.1.3	Publicación de manuales y documentos aprobados.		R	R	P
1.2.2	Definición de fundamentos del SGSI.				
1.2.2.1	Definir el alcance del SGSI.	A	R		
1.2.2.2	Definir los objetivos estratégicos de la política de seguridad.	A	R		

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1.2.2.3	Manual de gestión de seguridad de la información.				
1.2.2.3.1	Manual de auditoria de sistemas.	V	R	R	P
1.2.2.3.2	Manual de gestión de riesgos.	V	R	R	P
1.2.2.3.3	Manual de control de documentos.	V	R	R	P
1.2.2.3.4	Manual de mejora continua.	V	R	R	P
1.3	Diagnóstico del SGSI - carta de aplicabilidad SGSI.				
1.3.1	Aprobación de la declaración de aplicabilidad.	A	R	R	P
1.3.2	Generar "declaración de aplicabilidad".	A	R	R	P
1.4	Diagnóstico del SGSI - análisis de riesgos.				
1.4.1	Tratamiento de riesgos.				
1.4.1.1	Carta de aceptación de riesgos por parte de la alta gerencia.	A	R		
1.4.1.2	Plan de tratamiento de riesgos.				
1.4.1.2.1	Aprobación del plan de tratamiento de riesgos.	A	R	P	P
1.4.1.2.2	Preparación de los procedimientos para implantar los controles.		A	R	P
1.4.1.2.3	Selección de los controles de la norma ISO 27002.		A	R	P
1.4.2	Estimación de riesgos.				
1.4.2.1	Revisión y confirmación de factores de riesgo.	A	R	P	P
1.4.2.2	Documento de probabilidad e impacto de factores de riesgo.	A	R	P	P

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1.4.2.3	Estimar y validar tamaño y complejidad de los factores de riesgo.				
1.4.2.3.1	Cálculo del valor de riesgo asociado a cada activo.	A	R	v	P
1.4.2.3.2	Identificación y evaluación de amenazas y vulnerabilidades de los activos.	A	R	v	P
1.4.3	Identificación de riesgos para cada activo de información.	A	R	v	P
1.4.4	Identificación de los procesos de la cadena de valor de la organización.	A	R	v	P
1.4.5	Inventario de activos de la información.	A	R	v	P
1.5	Capacitación.				
1.5.1	Formación y entrenamiento.	A	R	P	
1.5.2	Definición del calendario de formación y entrenamiento.	A	R	P	
1.5.3	Preparación del material de formación y entrenamiento.	A	R	P	
1.6	Implementación del SGSI.				
1.6.1	Organización de la seguridad de la información.				
1.6.1.1	Entrenamiento y entendimiento de los controles.	A	R	P	
1.6.1.2	Aprobar y publicar controles y procedimientos.	A	R	P	
1.6.1.3	Aplicación de controles.				
1.6.1.3.1	Gestión de las comunicaciones y la operación.	A	R	P	
1.6.1.3.2	Control de acceso.	A	R	P	

Entregables		Roles			
EDT	**Nombre de tarea**	**PA**	**GP**	**AS II**	**AS I**
1.6.1.3.3	Sistemas de información, adquisición, desarrollo y mantenimiento.	A	R	P	
1.6.1.3.4	Seguridad de la información en la gestión de incidentes.		A	R	P
1.6.1.3.5	Cumplimiento.	A	R	V	P
1.6.1.3.6	Gestión del plan de continuidad de negocio.	A	R	P	
1.6.1.3.7	Seguridad física y ambiental.	A	R	R	P
1.6.1.3.8	Seguridad del recurso humano.	A	R	R	P
1.6.2	Políticas de seguridad.				
1.6.2.1	Socialización y formación.	A	R	R	P
1.6.2.2	Aprobación de la política de seguridad.	A	R	R	P
1.6.2.3	Implementación de los controles.	A	R	R	P

Códigos de Responsabilidad		Código de Roles	
A	Aprueba el entregable	PA	Patrocinador
R	Responsible del entregable	GP	Gerente del Proyecto
P	Participa	AS II	Asesor Nivel II
V	Revisa	AS I	Asesor Nivel I

Fuente: Autores del texto

Criterios de liberación del personal del proyecto:

A continuación se puede observar cuando se libera los recursos y el destino de cada uno de ellos cuando cumplen su rol en el proyecto.

Rol	Criterio de liberación	¿Cómo?	Destino de asignación
Patrocinador	Al terminar el		Otro proyecto en

Rol	Criterio de liberación	¿Cómo?	Destino de asignación
	proyecto		Fullcarga
Director del proyecto	Al terminar el proyecto	Comunicación del patrocinador	Otro proyecto en Fullcarga
Asesor nivel II	Al terminar el proyecto	Comunicación del director del proyecto	
Asesor nivel I	Al terminar el proyecto	Comunicación del director del proyecto	
Departamento de tecnología	Al terminar el proyecto	Coordinación del patrocinador	

Fuente: Autores del texto

Capacitaciones

1. El personal de la compañía Fullcarga Colombia debe aprovechar toda capacitación presentada en la compañía relacionada al tema de sistema de gestión de seguridad de la información y gestión de calidad para generar una mejora continua a los procesos de la compañía.
2. Se debe aprovechar los proyectos internos, para que los gerentes de proyectos reciban experiencia y poder desarrollar sus habilidades de gestión de proyectos.

Sistema de reconocimientos y recompensas

El director del proyecto tiene un sistema de incentivo por cumplimiento al proyecto:

1. El indicador de gestión de costos al finalizar el proyecto entre 0,95 y 1, recibiría un 20% de bono sobre remuneración mensual durante el plazo del proyecto.

2. El indicador de gestión de tiempo al finalizar el proyecto menor que 1, recibiría un 20% de bono sobre remuneración mensual durante el plazo del proyecto.
3. Cualquier incumplimiento de cualquiera de los dos indicadores de gestión anula cualquier otro bono.

Cumplimiento de regulaciones, pactos y políticas

1. Solo se debe contratar asesores que tengan la certificación de auditor interno de ISO 27001:2005
2. Todo personal de la empresa que participa del proyecto pasara por una evaluación de desempeño al final del proyecto, y dicha evaluación se guardara en su archivo personal.

PLAN DE GESTIÓN DE ADQUISICIONES[6]

Los ítems del plan de gestión de adquisiciones son los siguientes:

1. Procedimiento estándar a seguir:

A continuación se presentará los procedimientos para todo tipo de adquisición de recurso para el proyecto.

Para los contratos de personal del proyecto:

- Solicitar al departamento de recursos humanos de la compañía la contratación del personal según el perfil del plan de gestión de recursos humanos.
- Para el caso de los asesores nivel I y II, después de hacer el proceso interno del departamento de recursos humanos serán entrevistados por el Director del Proyecto quien puede hacer la selección del personal.
- Para el caso del director de proyecto, será entrevistado por el patrocinador, después de haber concluido el proceso interno de recursos humanos.
- Para el formato del contrato se utilizara el definido por el de la compañía FullCarga Colombia S.A.

Para las adquisiciones de materiales se tiene proveedores selecciones por la compañía:

- Para el caso de los equipos portátiles hacer el requerimiento al departamento de compras, para que se contacte con los proveedores y solicitar la cotización con los requerimientos necesitados.
- Para el caso de los equipos móviles hacer el requerimiento al departamento de compras, para que se contacte con los proveedores y solicitar la cotización con los requerimientos necesitados.

[6] Se tomó como base de desarrollo el modelo, recomendaciones y formatos expuestos por Darma Consulting: ***http://dharmacon.net/site/***

- En el caso de los materiales como son: CD's, hojas, tintas, etc., se solicita la cotización de tales productos en la cantidad necesaria.
- Para la compra de la cartilla ISO 27001:2005 se hace el requerimiento al departamento de compras la cual debe ser adquirida de www.iso.org

2. Formatos estándar a utilizar

- Fullcarga Colombia S.A. tiene un formato de contratación, el cual es el que se va a utilizar en el proyecto para la adquisición de personal.
- Fullcarga Colombia S.A. tiene un formato para requerimiento de insumos el cual es el que se va a utilizar en el proyecto.

3. Restricciones y supuestos:

Las restricciones y/o supuestos que han sido identificados y que pueden afectar las adquisiciones del proyecto son:

- Solicitudes de cambio en el presupuesto del proyecto, debido a que el personal según el perfil no esté disponible en el mercado o su aspiración salarial sea mayor a la ofrecida. Este será evaluado por el director del proyecto y el patrocinador.
- Se asume que la probabilidad de modificación del cronograma es mínima, debido a que un aplazamiento conlleva una extensión del contrato del personal.

4. Riesgos y repuestas

Según el plan de gestión de riesgos se tiene lo siguiente se identificó los siguientes:

- R02 - Bajas en el equipo de desarrollo
    - Reasignar tareas al personal de equipo y distribuir tiempos para no dejar inconcluso el desarrollo del proyecto
    - Realizar el requerimiento a recursos humanos con prioridad para completar el equipo de trabajo.

5. Métricas

Se tomará como referencia la medición de métricas de costos del proyecto, que se tiene en el aseguramiento de la calidad.

PLAN DE GESTIÓN DE RIESGOS

Uno de los elementos clave a la hora de asegurar el éxito en el proyecto, medido en términos de cumplimiento de plazos, costes, alcance funcional y calidad final de la solución, es la gestión de riesgos.

Implementar la gestión de riesgos correcta es un elemento decisivo a la hora de asegurar el proyecto, mediante la identificación y el análisis de los riesgos potenciales que puedan afectar al proyecto y el establecimiento de acciones de contingencia para evitar su aparición o para minimizar el impacto en el Proyecto, en caso de que finalmente el riesgo se verifique.

Propósito

Este documento presenta el análisis de los riesgos identificados durante la fase de Inicio del proyecto “aseguramiento de la información en el proceso transaccional de recarga electrónica”. Para cada riesgo observado se valorarán sus efectos y contexto de aparición para el caso en que se convierta en un hecho; además, se definirán estrategias para reducir la probabilidad del riesgo o para controlar sus posibles efectos.

Alcance

El ámbito del análisis de riesgos cubre toda la extensión del proyecto observado desde su fase inicial. Será necesario durante el desarrollo del proyecto revisar y actualizar los contenidos del análisis de riesgos en caso de que se detecten nuevos riegos no visibles en este momento.

Este documento será aplicable a todas las fases del Proyecto.

Gestión del riesgo

A continuación se podrá observar la identificación de los riesgos (Ilustración 44), el análisis de riesgo (Ilustración 45), las acciones preventivas y correctivas

de cada uno de ellos (Ilustración 46) y los responsables de control y seguimiento del riesgo de los proyectos (Ilustración 47).

Ilustración 44. Identificación de riesgos

ID	Descripción del riesgo	Tipo de riesgo
R01	Requisitos poco claros	Riesgo del proyecto
R02	Abandono temporal de un miembro del equipo	Riesgo del proyecto
R03	Falta de experiencia en tareas de planificación	Riesgo del proyecto
R04	Falta de experiencia con las herramientas utilizadas	Riesgo del producto/proyecto
R05	Diseño erróneo	Riesgo del producto
R06	Falta de un experto	Riesgo del proyecto
R07	Pérdida de documentación y/o otros artefactos	Riesgo del proyecto
R08	Conflictos entre los integrantes del grupo	Riesgo del proyecto
R09	Inestabilidad del entorno de desarrollo y documentación el proyecto	Riesgo del proyecto
R10	Estimación de costos fuera del alcance de la realidad	Riesgo del proyecto
R11	Falta de seguimiento permanente de tareas y actividades	Riesgo del proyecto
R12	Falta de comunicación entre los integrantes del grupo.	Riesgo del proyecto
R13	Afectación de los equipos (virus, software desactualizado).	Riesgo del producto

Fuente: Autores del texto

Ilustración 45. Análisis de riesgo

ID	Análisis del riesgo
R01	**Magnitud** Variable según la fase de aparición: ▪ Inicio: baja. ▪ Elaboración: media. ▪ Construcción: alta. ▪ Transición: muy alta **Descripción** Descripción detallada de los requisitos del proyecto.

ID	Análisis del riesgo
	Impacto Si los requisitos iniciales del proyecto se modifican, se deberá afectar directamente los criterios de alcance, tiempo o recurso. **Indicadores** Número total de requerimientos finalizados, sobre el número total de requerimientos del proyecto.
02	**Magnitud** Alta: un miembro del equipo de trabajo. Muy Alta: se afecta a más de un miembro de trabajo. **Descripción** Se presenta ausencia de algún miembro de trabajo. **Impacto** Se presentará afectación del plan de trabajo, se puede requerir planes de emergencia o cambios en recurso o tiempo. **Indicadores** Número de horas hombre disponible dividido por el número de horas hombre requerido.
R03	**Magnitud** Media. **Descripción** El grupo tiene poca experiencia en el desarrollo de “aseguramiento de la información en el proceso transaccional de recarga electrónica software siguiendo una estructura de tareas y fechas preestablecido. **Impacto** La planificación guía todo el desarrollo del proyecto. Un error puede incidir directamente en sus resultados. No obstante, la división en iteraciones reduce el impacto de los errores, permitiendo que estos puedan ser corregidos o absorbidos en iteraciones posteriores a la de su aparición. **Indicadores** Diferencias entre el desarrollo real del proyecto y la planificación estimada.
R04	**Magnitud** Variable según la fase de aparición: ▪ Inicio: baja. ▪ Elaboración: media. ▪ Construcción: alta. ▪ Transición: alta. **Descripción** Falta de conocimiento, experiencia, habilidad para realizar las actividades requeridas para el proyecto por los integrantes del equipo de trabajo.

ID	Análisis del riesgo
	Impacto Puede suponer retrasos. Puede afectar la línea base del proyecto. **Indicadores** No Aplica.
R05	**Magnitud** Baja en elaboración, alta en construcción. **Descripción** El diseño del sistema resulta inadecuado. Al realizar actividades de implementación puede encontrase que el diseño carece del suficiente nivel de detalle o está mal enfocado, bien por la naturaleza del problema, o bien por restricciones de uso impuestas por terceros. **Impacto** Puede introducir retrasos en el proyecto ante la necesidad de volver a considerar el diseño trazado. Requiere la actualización o modificación de los artefactos de diseño. **Indicadores** No Aplica
R06	**Magnitud** Media. **Descripción** No hay un experto en el equipo de desarrollo al que poder consultar. **Impacto** Puede suponer retrasos. **Indicadores** No procede
R07	**Magnitud** Alta. **Descripción** Pérdida o inexistencia de la documentación requerida para la correcta ejecución del proyecto. Uso y resguardo inadecuado de los artefactos del proyecto. **Impacto** Variable, puede generar un retraso. **Indicadores** Ninguno.
R08	**Magnitud** Media. **Descripción** No lograr tener una conciliación clara en la toma de decisiones. **Impacto** Retraso en el desarrollo del plan de trabajo.

ID	Análisis del riesgo
	Indicadores Mucho tiempo dedicado a decisiones concretas, énfasis en las posturas enfrentadas, número de enfrentamientos con respecto a una misma decisión.
R09	**Magnitud** Alta **Descripción** Tanto el proceso de desarrollo como el de documentación puede sufrir caídas y/o variaciones intermitentes. **Impacto** Puede generar desconfianza en cuanto a la calidad del producto. **Indicadores** No Aplica
R10	**Magnitud** Media **Descripción** Se sobreestiman o subestiman los costos involucrados con el desarrollo del producto. **Impacto** Puede generar que el equipo entre en períodos de sobrecarga de trabajo o periodos de ausencia del mismo, lo que a su vez puede conllevar a un deterioro en la calidad **Indicadores** El equipo trabaja más o menos horas de las inicialmente programadas, se presentan quejas a jefe del proyecto.
R11	**Magnitud** Media **Descripción** No se realiza un seguimiento de las tareas planificadas, lo que puede ocasionar que algunas de ellas sean dejadas para última instancia, con la consecuente baja en su calidad **Impacto** Sobrecarga de trabajo en los días previos a la entrega de un presentable, pobre calidad de los entregables, se obvian detalles importantes. **Indicadores** No Aplica

ID	Análisis del riesgo
R12	**Magnitud** Alta **Descripción** El sistema se va a construir usando el lenguaje JSF. Los miembros del equipo de desarrollo tienen que aprender a utilizarlo. Un desconocimiento del sistema impedirá el desarrollo de la fase de construcción y elaboración de una manera ágil. **Impacto** Puede generar retrasos así como también que se vuelvan a desarrollar módulos que ya se encontraban terminados. **Indicadores** No procede
R13	**Magnitud** Media **Descripción** Durante la realización de un proyecto *software*, hay muchos artefactos y tareas que completar por la totalidad de integrantes del grupo. Normalmente dichas tareas están relacionadas de alguna manera, y cualquier cambio independiente en una de ellas afecta al resultado final o a otras tareas. **Impacto** Pueden producirse duplicación de tareas. **Indicadores** No Aplica.

Fuente: Autores del texto

Ilustración 46. Acciones de prevención y de corrección

ID	Plan de prevención	Plan de corrección
R01	Realización de varias reuniones; elaboración de cuestionarios para aclarar puntos poco claros de las reuniones previas.	Se evaluará y analizará los requisitos actuales del proyecto, generando nuevas especificaciones para determinar los requisitos del proyecto y aclararlos frente a todos los involucrados.

ID	Plan de prevención	Plan de corrección
		En caso de que se decida aceptar los cambios, se revisarán los requisitos afectados, así como toda la documentación y código derivado de los mismos hasta el punto de aparición del cambio.
R02	Tratar de cumplir las metas y objetivos antes de lo estimado en la planificación siempre que sea posible, para que una ausencia no suponga un retraso importante.	El equipo de desarrollo tratará de cubrir el trabajo no realizado por el miembro del proyecto que no puede trabajar. En caso necesario, dejarán de realizarse tareas menos importantes para centrarse en las principales. Se tratará de reajustar la planificación del proyecto.
R03	Realización de reuniones entre los miembros del proyecto para la evaluación de la marcha del proyecto y consultas requeridas.	Se observarán las diferencias entre la planificación de cada iteración y el informe de seguimiento de su ejecución, analizando las causas de sus diferencias para tratar de detectar y corregir errores de planificación en las iteraciones posteriores.
R04	Una parte del tiempo de desarrollo del proyecto se destinará al aprendizaje de las nuevas herramientas.	Si se produce un retraso en el aprendizaje por parte de un miembro del equipo, los demás miembros tratarán de ayudar a superarlo. Si no resultara, consultar a fuentes externas. En

ID	Plan de prevención	Plan de corrección
		último lugar se haría una redistribución de tareas.
R05	Durante la fase de elaboración se desarrollará en paralelo un prototipo conteniendo la arquitectura del sistema para comprobar la validez de la misma. En caso de encontrase errores o inconsistencias, podrá modificarse el diseño al mismo tiempo que la implementación del prototipo.	Si el riesgo se convierte en hecho durante la fase de Elaboración, se revisará y modificará la documentación de diseño afectada. Si lo hace durante la fase de construcción, se estudiará una solución acorde a los tiempos de plazo de que se dispone. La planificación se reajustará si fuera necesario.
R06	Aprendizaje continuo durante todo el proyecto	Las dudas que no se sepan resolver se trasladarán y/o suben hasta obtener la solución.
R07	Se realizarán copias de seguridad de la información de cada uno de los miembros del equipo, así como copias en un servidor remoto	Actualizar con la última copia disponible
R08	Cada vez que se fije un punto de dirección en el proyecto, todo tiene que quedar totalmente claro, sin dudas y con la aceptación total de todos los miembros del grupo.	Se establecen reglas para definir una política de toma de decisiones en caso de desacuerdo. Las cuestiones de diseño o técnicas se tratarán junto al tutor del proyecto, que aportará su opinión.
R09	Disponer de equipos adicionales	Tener todo el tiempo *Backup* de

ID	Plan de prevención	Plan de corrección
		la información.
R10	Realizar estimaciones en base a varias herramientas para tratar de hallar un estimado más cercano a la realidad	Redimensionar el proyecto conforme se va desarrollando y nuevas funcionalidades se agregan o se eliminan.
R11	Llevar al día una revisión del estado del proyecto para anotar los posibles atrasos y poder así tomar medidas en el instante.	Realizar un nuevo direccionamiento de tareas, así como llamadas de atención a los miembros del equipo que dejen sus tareas para última instancia.
R12	Se ha de conseguir bibliografía básica y realizar un taller entre los integrantes del grupo.	En caso de que el aprendizaje sea demasiado costoso, la tecnología de programación de "salvaguarda" será PHP.
R12	Mantener una documentación única como medio de documentación centralizado.	Realizar reuniones para acordar temas referentes al proyecto así como las fechas de futuras reuniones.

Fuente: Autores del texto

Ilustración 47. Control y seguimiento de riesgos

Id.	Responsable	Fecha de terminación	Estado	Observaciones
R01	Auditor	Fin del proyecto	Iniciado	
R02	Jefe de Proyecto	Fin del proyecto	Iniciado	
R03	Jefe de Proyecto	Fin del proyecto	Iniciado	

R04	Equipo de desarrollo	Fin del proyecto	Iniciado	
R05	Auditor	Fin del proyecto	Iniciado	
R06	Equipo de desarrollo	Fin del proyecto	Iniciado	
R07	Equipo de desarrollo	Fin del Proyecto	Iniciado	
R08	Equipo de desarrollo	Fin del proyecto	Iniciado	
R09	Equipo de desarrollo	Fin del proyecto	Iniciado	
R10	Auditor	Fin del proyecto	Iniciado	
R11	Jefe del proyecto	Fin del proyecto	Iniciado	
R12	Equipo de desarrollo	Fin del proyecto	Iniciado	

Fuente: Autores del texto

Responsable: Persona o personas asignadas a la implantación de las acciones preventivas y/o correctoras

Fecha Terminación: Fecha límite en la cual todas las acciones anteriormente descritas deban haber sido ejecutadas por el responsable o responsables asignados.

Estado: Estado actual del riesgo y de las acciones preventivas y/o correctoras.

Observaciones: Descripción de las observaciones encontradas para este riesgo (opcional).

Matriz de riesgo

Se propone la utilización de una matriz específica que sirva de soporte para la gestión de Riesgos. Esta matriz (Ilustración 48) se utilizará en las reuniones de seguimiento y/o cuando se estime necesario (en el caso de situaciones excepcionales), y su contenido será el siguiente:

Ilustración 48. Matriz de riesgo

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
R01	1.4, 1.5	Cambios en los requisitos	Producto	20	4	0,8	Realización de varias reuniones con el cliente para la aclaración de requisitos.	Se revisarán los requisitos afectados, así como toda la documentación y código derivado de los mismos hasta el punto de aparición del cambio.
R02	1.4, 1.5	Bajas en el equipo de desarrollo	Proyecto	30	4	1,2	Tratar de cumplir las metas y objetivos antes	Reasignar ciertas tareas a otros miembros según

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
							de lo estimado en la planificación siempre que sea posible.	vayan siendo necesarios los artefactos para la consecución de los hitos.
R03	1.2, 1.3, 1.5	Falta de experiencia en tareas de planificación	Proyecto	50	2	1	Realización de reuniones entre los miembros del proyecto para la evaluación de la marcha del proyecto.	Se observarán las diferencias entre la planificación de cada iteración y el informe de seguimiento, para tratar de detectar y corregir errores de planificación en iteraciones posteriores.
R04	1.2.1,	Falta de	Producto/pro	50	2	1	Una parte del	Si se produce un

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
	1.3.1.2	experiencia con las herramientas utilizadas	yecto				tiempo de desarrollo del proyecto se destinará al aprendizaje de las herramientas de documentación e implementación.	retraso por parte de un miembro del equipo, los demás miembros tratarán de ayudar a superarlo. Consultar a fuentes externas en último lugar, se haría una redistribución de tareas.
R05	1.2	Diseño Erróneo	Producto	40	3	1,2	Durante la fase de Elaboración se desarrollará en paralelo un prototipo conteniendo la estructura del	Se revisará y modificará la documentación de diseño afectada. La planificación se reajustará si fuera necesario.

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
							sistema para comprobar la validez de la misma.	
R06	1.2, 1.3, 1.4, 1.5	Falta de un experto	Proyecto	80	1	0,8	Aprendizaje continuo durante todo el proyecto	Las dudas que no se sepan resolver se trasladarán al tutor y a foros especializados.
R07	1.3, 1.5, 1.4	Pérdida de documentación y/o otros artefactos	Proyecto	40	4	1,6	Se usará un repositorio, para el control de versiones. Se realizarán copias de seguridad en los ordenadores personales de cada uno de los	Actualizar con la última copia disponible

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
							miembros del equipo de desarrollo.	
R08	1.1	Conflictos entre los integrantes del grupo	Proyecto	75	2	1,5	Se celebrarán reuniones de proyecto para poder discutir cuestiones de requisitos y diseño.	Establecer las reglas para definir una política de toma de decisiones en caso de desacuerdo.
R09	1.2, 1.3	Inestabilidad del entorno de desarrollo y documentación el proyecto	Proyecto	80	5	4	Asegurar una empresa que brinde garantía de su servicio	Utilizar una de las computadoras del equipo como servidor.
R10	1.2, 1.3,	Mala estimación de	Proyecto	50	3	1,5	Realización de varias	Redimensionar el proyecto conforme

Id.	EDT	Descripción del riesgo	Tipo riesgo	Probabilidad de ocurrencia	Impacto	Evaluación del riesgo	Acciones de prevención	Acción de corrección
	1.4, 1.5	costos					estimaciones con metodologías diferentes	se ejecuta
R11	1.4, 1.3	Falta de seguimiento de tareas	Proyecto	50	3	1,5	Planificación adecuada de tareas, seguimiento del desarrollo de las mismas.	Charla con el equipo de desarrollo en caso de detectarse malas prácticas.
R12	1.1	Falta de Comunicación entre los Integrantes	Proyecto	20	2	0,4	Mantener una documentación única como medio de documentación centralizado.	Realizar reuniones informativas

Fuente: Autores del texto

Id.: Identificador de Riesgo

Descripción del Riesgo: Descripción resumida del riesgo

Probabilidad (1 a 100): Grado de probabilidad de que el riesgo finalmente se produzca. Se mide en una escala de 1 a 100 (porcentual).

Nivel de Impacto: Grado de impacto en el proyecto en el caso de que el Riesgo finalmente se produjera. Se mide en una escala de 1 a 5, siendo 1=poco influyente hasta 5=fuertemente influyente.

Probabilidad Ocurrencia: Valor numérico resultante del producto del grado de probabilidad por el grado de impacto. Este producto dará la prioridad que tendrá la gestión de este riesgo y la implantación de sus medidas preventivas o correctoras.

Acciones Prevención: Descripción de las acciones o medidas a adoptar para evitar (mitigar) la aparición final del riesgo

Acciones Corrección: Descripción de las acciones o medidas a adoptar en el caso en el que el riesgo finalmente se haya producido.

PLAN DE GESTIÓN DE COMUNICACIONES

Para el proyecto se utilizará diferentes medios de comunicación, se deberá establecer un canal único y un procedimiento claro para el manejo de conflictos; se establecerán reuniones de seguimiento semanal entre los integrantes de tabajo y reportes mensuales a la alta gerencia.

Se utilizará metodología Scrum-Kambal para el control de las actividades de los diferentes equipos, que serán la fuente de información para los cuadros de mando requeridos para el control por parte del Gerente de proyecto

1.1. Restricciones

Se utilizará para la comunicación directa la aplicación *Outlook* versión 2007 y de cada acta se deberá generar un acta en un formato estándar y se debe publicar en PDF en SharePoint del proyecto.

1.2. Distribución de la Información

Se deberá seguir la matriz de comunicaciones relacionada a continuación para la distribución de la información:

Matriz de comunicación		Alcance del proyecto /Solicitudes Cambio	Soporte de admón./ avance/ informes de rendimiento	Datos actuales del proyecto	Diseños	Coordinación	Avance / Necesidad de recursos	Avance/ requerimientos	Aceptación del proyecto
Involucrado	**Rol en el proyecto**	Quincenal	Constante	Semanal	Diaria	Según requerimiento	Inicial/ requeriré	Inicial requerido	Inicial requerido
Jairo Melo	Director del proyecto	**X**		**X**		**X**	**X**	**X**	**X**
----------	Asesor Nivel I		**X**	**X**		**X**			
Daniel Gutiérrez	Asesor Nivel II		**X**	**X**		**X**			
----------	Departamento de tecnología	**X**		**X**			**X**		**X**
----------	*Chief Information Officer*	**X**	**X**		**X**		**X**	**X**	**X**

Fuente: Autores del texto

2.3 Proceso de lecciones aprendidas

El equipo de dirección de proyectos desarrollará y archivará las lecciones aprendidas cada semana, para actualizar los activos. El equipo de dirección de proyecto deberá mantener un archivo de documentos tales como:

- Documentos recibidos: Documentos generales de importancia media a baja por parte de los involucrados del proyecto y ordenar por fecha.
- Documentos enviados: Documentos generales de importancia media a baja por parte de los involucrados del proyecto y ordenar por fecha.
- Permisos obtenidos: Recepción de permisos de las instituciones gubernamentales involucradas. (si aplica)
- Ofertas o cotizaciones de empresas.
- Minutas de reuniones: Minutas de reuniones semanales o mensuales.
- Solicitudes de cambio en general: Documentar las solicitudes (enumeradas) de cambio aprobadas separadas de las no aprobadas y llevar una lista de resumen que facilite el acceso y conocimiento de las mismas.
- Informes: Documentar informes de avance y rendimientos.
- Tablas de pago: Tabla de pagos separados por empresa.
- Plan de gestión actualizado y detalle resumido de cambios actualizados: archivar de manera consecutiva los cambios que se vayan generando respecto al plan de gestión inicial, de esta manera, se podrá mejorar en algunos casos, futuros planes de gestión.

Bibliografía

Avance Jurídico Casa Editorial Ltda. (5 de Enero de 2009). *Senado de la República de Colombia*. Recuperado el 22 de Marzo de 2013, de LEY 1273 DE 2009: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

Banco de la Republica de Colombia. (Julio de 2006). *Tasa de rendimiento de capital de Colombia*. Recuperado el 15 de Mayo de 2015, de http://www.banrep.gov.co/es/borrador-398

Blog-Top Punto Com. (14 de Julio de 2007). *Blog-Top Punto Com*. Recuperado el 22 de Marzo de 2013, de Blog-Top Punto Com: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

Borbon Sanabria, J. S. (25 de Julio de 2011). *.Seguridad*. Recuperado el 20 de Julio de 2012, de .Seguridad: http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

EL TIEMPO casa editorial. (s.f.). *ELEMPLEO.com*. Recuperado el 23 de Junio de 2012, de ELEMPLEO.com: http://www.elempleo.com/colombia/herramientas/calculadora-salarial

EMAGISTER. (2010). *EMAGISTER*. Recuperado el 23 de Junio de 2012, de EMAGISTER: http://www.emagister.com.co/certificacion-iso-27001-tps-77309.htm

FULLCARGA COLOMBIA S.A. (2011). *ESTUDIO DE MERCADO CONSULTORIA ISO 27001.* BOGOTÁ.

FULLCARGA COLOMBIA S.A. (2012). *CENTRO DE COSTOS.* BOGOTA.

FullCarga Internacional. (Enero de 2011). Presentación comercial 2011. Bogotá, Colombia.

GES CONSULTOR. (03 de Abril de 2013). *ISO 27001 – Sistema de Gestión de la Seguridad de la Información*. Recuperado el 15 de Junio de 2013, de ISO 27001 – Sistema de Gestión de la Seguridad de la Información: http://www.gesconsultor.com/iso-27001.html

Goedkoop, M., Effting, S., & Collignon, M. (5 de Noviembre de 1999). *Manual práctico de ecodiseño.* Recuperado el 15 de Junio de 2013, de Manual práctico de ecodiseño:

http://www.lapetus.uchile.cl/lapetus/archivos/112_Manual_practico_Eco_indicador_99.pdf

Hernandez, C. (Junio de 2010). *Monografías*. Recuperado el Julio de 2012, de Monografías: http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml

Holland & Holland Enterprise. (2010). *Succesful project management*. Recuperado el 25 de Julio de 2012, de Succesful project management: http://www.successful-project-management.com/resource-breakdown-structure.html

ISO. (Julio de 2007). *Wordpress.* Recuperado el Julio de 2012, de Wordpress: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

ISO. (2008). *The ISO 27000 Dictionary.* Recuperado el Julio de 2012, de The ISO 27000 Dictionary: http://www.27000.org/iso-27005.htm

ISO/IEC. (15 de Junio de 2005). *Wordpress.* Recuperado el Julio de 2012, de Wordpress: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Marblestation. (Marzo de 2008). *Marblestation*. Recuperado el Julio de 2012, de Marblestation: http://www.marblestation.com/?p=650

Ministerio de Minas y Energía de Perú. (2010). *Ministerio de Minas y Energía de Perú*. Recuperado el 2013 de Junio de 20, de Ministerio de Minas y Energía de Perú: http://intranet.minem.gob.pe/AppWeb/DGE/CalculoConsumo

Real Academia Española. (s.f.). *Diccionario de la Lengua Española*, 22a. Recuperado el 16 de Febrero de 2013, de www.rae.es: http://lema.rae.es/drae/?val=seguridad

Román, P. (29 de Octubre de 2010). *Cibercultural*. Recuperado el 23 de Marzo de 2013, de http://cibercultural.wordpress.com/2010/10/29/la-influencia-de-las-tics-en-la-sociedad/

Superintendencia Financiera de Colombia. (30 de 09 de 2014). *Reporte de Inclusión Financiera.* Recuperado el 12 de 05 de 2015, de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=10083368

UN Publications. (2000). *www.un.org*. Recuperado el 25 de Octubre de 2013, de www.un.org: http://www.un.org/es/millenniumgoals/

UN Publications. (8 de Septiembre de 2000). *www.un.org*. Recuperado el 25 de Octubre de 2013, de www.un.org: http://www.un.org/spanish/milenio/ares552s.htm

Vargas, L. (2011). *Monografías.* Recuperado el Julio de 2012, de Monografías: http://www.monografias.com/trabajos38/cobit/cobit.shtml

Anexo 1. Técnica nominal de grupo

TÉCNICA NOMINAL DE GRUPO

Nombre del proyecto:

Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.

Temas de decisión:

Para la selección de los criterios de decisión de las alternativas de solución se tuvo en cuenta los siguientes parámetros: alcance, tiempo, costo, impacto, calidad, teniendo cada uno de estos factores el 20% de participación exceptuando tiempo y costos que tienen 10% y 30% respectivamente.

Aplicación de la técnica nominal de grupo (1 es no favorable y 10 favorable

	Alcance 20%			
Alternativa	DG	JM	BB	Total
Alternativa 1	9	8	8	25
Alternativa 2	7	8	9	24
Alternativa 3	6	6	6	18

	Tiempo 10%			
Alternativa	DG	JM	BB	Total
Alternativa 1	9	9	9	27
Alternativa 2	9	9	9	27
Alternativa 3	7	8	6	21

	Costo 30%			
Alternativa	DG	JM	BB	Total
Alternativa 1	6	7	5	18
Alternativa 2	8	9	8	25
Alternativa 3	7	5	6	18

	Impacto 20%			
Alternativa	DG	JM	BB	Total
Alternativa 1	8	9	8	25
Alternativa 2	9	9	8	26
Alternativa 3	7	7	6	20

	Calidad 20%			
Alternativa	DG	JM	BB	Total
Alternativa 1	6	4	5	15
Alternativa 2	7	8	7	22
Alternativa 3	3	4	2	9

Total

Alternativa	Alcance	Tiempo	Costo	Impacto	Calidad	Total
Alternativa 1	5	2,7	5,4	5	3	21,1
Alternativa 2	4,8	2,7	7,5	5,2	4,4	24,6
Alternativa 3	3,6	2,1	5,4	4	1,8	16,9

Anexo 2. Project Charter

PROJECT CHARTER

Nombre del proyecto:

Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.

Descripción general del proyecto:

Fullcarga Colombia está planeando en certificarse en ISO 27001:2005 y quiere definir la brecha que tiene el proceso frente a la norma.

Propósito del project charter:

El propósito del *project charter* es proveer un mejor entendimiento del proyecto, establecer un alcance general y definir los niveles de autoridad.

Objetivo del proyecto:

Definir el plan de trabajo del Sistetma de Gestion de Seguridad de la Información; mediante el que Fullcarga establezca una metodología y los controles requeridos para operar, monitorear, revisar, mantener y mejorar el proceso transaccional de recarga en línea.

Alcance del proyecto:

Identificar la brecha de controles de seguridad de la información teniendo en cuenta los dominios de seguridad existentes frente a la norma ISO 27001:2005 y definir el plan de acción. No se contempla en el desarrollo de este proceso de establecer controles y la ejecución de los mismos.

Hitos importantes

Recolección de Información del proceso actual
Estudio de actual de la brecha del sistema frente a la norma
Análisis de Riesgos
Definición de los planes de control

Entregables importantes

Diagnóstico
Evaluación de riesgos
Planeación SGSI
Planes de control de aseguramiento de información

Supuestos

No se requerirá hacer nuevas oficinas en el proyecto
Los empleados de la compañía pueden hacer sugerencias mediante el buzón de PQR
Todo el personal de Fullcarga están dispuesto al cambio y mejora continua
Se harán avances semanales del proyecto.

Limitaciones

Disponibilidad limitada del área de departamento técnico.
Resistencia al cambio
Prioridad en otros proyectos de la compañía.

Oportunidad de negocio

El propósito de este proyecto es buscar la certificación ISO 27001:2005 generando valor agregado en el manejo de la información frente a entes de control financiero.

Costos preliminares del proyecto

El proyecto va tener unos costos aproximados de COP $150.000.000 (Ciento cincuenta millones de pesos m/cte.)

Aceptación project charter

Beatriz Brum Chief Information Officer	Jairo Yesid Melo Gerente del Proyecto

Anexo 3. Project scope statement

PROJECT SCOPE STATEMENT

Nombre del proyecto:

Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.

Justificación:

La necesidad de este proyecto se genera en la compañía para poder tener clientes de la banca, demostrando confiabilidad en el manejo de los datos. Esto se realiza bajo los requerimientos de la ISO 27001:2005

Objetivo del proyecto:

Implementar un sistema de Seguridad de la Información por medio del Sistema de Gestión de Seguridad de la Información (SGSI); mediante el que Fullcarga establezca una metodología y los controles requeridos para operar, monitorear, revisar, mantener y mejorar el proceso transaccional de recarga en línea

Presupuesto del proyecto

Los honorarios estimados para la realización del proyecto en la fase de diagnóstico, tomando como base el equipo de trabajo propuesto serán de: COP $ 150.000.000. Se aproxima en un caso de negocio global cuyo proyecto tiene tres fases:
1. Diagnóstico, 2. Implementación y 3. Certificación un valor de COP $2.500.000.000.

Tiempo del proyecto

El proyecto en la fase de diagnóstico tiene un tiempo estimado de ocho (8) meses para su implementación.

Entregables del proyecto

Fase del proyecto	Producto entregable
1. Gestión de inicio SGSI	Manuales de auditorías, riesgos y control de cambios. *Kick off* del SGSI
2. Aplicabilidad SGSI	Carta de aplicabilidad del SGSI
3. Análisis de riesgos	Identificación y análisis de riesgos
4. Formación y sensibilización	Distribución de material de los manuales de calidad de SGSI y 2 sesiones de capacitación.
5. Preparación certificación	Material impreso del SGSI y una auditoria interna
6. Gerencia de proyectos	Proyecto gestionado

Supuestos del proyecto
No se requerirá hacer nuevas oficinas en el proyecto Los empleados de la compañía pueden hacer sugerencias mediante el buzón de PQR El cliente respetara el cronograma de trabajo del proyecto. Se cuenta con los asesores capacitados para el desarrollo del proyecto Todo el personal de Fullcarga están dispuesto al cambio y mejora continua
Restricciones del proyecto
El presupuesto no debe exceder lo presentado en la propuesta Se harán avances semanales del proyecto. Prioridad en otros proyectos de la compañía en el departamento de tecnología
Aceptación Project Scope Stament
Beatriz Brum — Chief Information Officer Jairo Yesid Melo — Project Manager

Anexo 4. Product Scope Statement

PRODUCT SCOPE STATEMENT

Nombre del proyecto:

Aseguramiento de la información en el proceso transaccional de recarga electrónica de la organización Fullcarga Colombia S.A.

Justificación:

La necesidad de este proyecto se genera en la compañía para poder tener clientes de la banca, demostrando confiabilidad en el manejo de los datos. Esto se realiza bajo los requerimientos de la ISO 27001:2005

Objetivo del proyecto:

Definir el plan de trabajo del Sistetma de Gestion de Seguridad de la Información; mediante el que Fullcarga establezca una metodología y los controles requeridos para operar, monitorear, revisar, mantener y mejorar el proceso transaccional de recarga en línea.

Descripción del alcance del producto

Identificar la brecha de controles de seguridad de la información teniendo en cuenta los dominios de seguridad existentes frente a la norma ISO 27001:2005 y definir el plan de acción. No se contempla en el desarrollo de este proceso de establecer controles y la ejecución de los mismos.

Entregables del proyecto

fase del proyecto	Producto entregable
1. Gestión de inicio SGSI	Manuales de auditorías, riesgos y control de cambios. *Kick off* del SGSI
2. Aplicabilidad SGSI	Carta de aplicabilidad del SGSI
3. Análisis de riesgos	Identificación y análisis de riesgos
4. Formación y sensibilización	Distribución de material de los manuales de calidad de SGSI y 2 sesiones de capacitación.
5. Preparación certificación	Material impreso del SGSI y una auditoria interna
6. Gerencia de proyectos	Proyecto Gestionado

Criterios de aceptación del producto	
1. Técnicos	La brecha del SGSI debe ser 100% identificada y con sus planes de mejora
2. De calidad	Se debe lograr el 90% de satisfacción del cliente
3. Administrativos	Todos los entregables serán revisados por el departamento de tecnología de FullCarga Colombia
4. Comerciales	Cumplir lo estipulado en el contrato
Aceptación Product scope stament	
Beatriz Brum Chief Information Officer	Jairo Yesid Melo Project Manager

Anexo 5. Autodiagnóstico de la ISO 27001

FORMULARIO PARA AUTODIAGNOSTICO DE SEGURIDAD FULLCARGA COLOMBIA
(BASADO EN LA NORMA ISO 27001)

POLÍTICAS DE SEGURIDAD

•Existen documento(s) de políticas de seguridad de SI	☑ VERDADERO
•Existe normativa relativa a la seguridad de los SI	☐ FALSO
•Existen procedimientos relativos a la seguridad de SI	☐ FALSO
•Existe un responsable de las políticas, normas y procedimientos	☑ VERDADERO
•Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO
•Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO

ORGANIZACIÓN DE LA SEGURIDAD

•Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☐ FALSO
•Existe un responsable encargado de evaluar la adquisición y cambios de SI	☑ VERDADERO
La Dirección y las áreas de la Organización participa en temas de seguridad	☐ FALSO
•Existen condiciones contractuales de seguridad con terceros y outsourcing	☑ VERDADERO
•Existen criterios de seguridad en el manejo de terceras partes	☑ VERDADERO
•Existen programas de formación en seguridad para los empleados, clientes y terceros	☐ FALSO
•Existe un acuerdo de confidencialidad de la información que se accesa.	☑ VERDADERO
•Se revisa la organización de la seguridad periódicamente por una empresa externa	☐ FALSO

ADMINISTRACIÓN DE ACTIVOS

•Existen un inventario de activos actualizado	☑ VERDADERO
•El Inventario contiene activos de datos, software, equipos y servicios	☐ FALSO
•Se dispone de una clasificación de la información según la criticidad de la misma	☐ FALSO
• Existe un responsable de los activos	☑ VERDADERO
•Existen procedimientos para clasificar la información	☐ FALSO
•Existen procedimientos de etiquetado de la información	☐ FALSO

SEGURIDAD DE LOS RRHH

•Se tienen definidas responsabilidades y roles de seguridad	☐ FALSO
•Se tiene en cuenta la seguridad en la selección y baja del personal	☐ FALSO
•Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☑ VERDADERO
•Se imparte la formación adecuada de seguridad y tratamiento de activos	☐ FALSO
•Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	☐ FALSO
•Se recogen los datos de los incidentes de forma detallada	☐ FALSO
•Informan los usuarios de las vulnerabilidades observadas o sospechadas	☐ FALSO
•Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	☐ FALSO
• Existe un proceso disciplinario de la seguridad de la información	☐ FALSO

SEGURIDAD FÍSICA Y DEL AMBIENTE

Existe perímetro de seguridad física(una pared, puerta con llave).	☑ VERDADERO
Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☐ FALSO
Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	☑ VERDADERO
En las áreas seguras existen controles adicionales al personal propio y ajeno	☐ FALSO
Las áreas de carga y expedición están aisladas de las áreas de SI	☑ VERDADERO
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	☑ VERDADERO
Existen protecciones frente a fallos en la alimentación eléctrica	☑ VERDADERO
Existe seguridad en el cableado frente a daños e intercepciones	☑ VERDADERO
Se asegura la disponibilidad e integridad de todos los equipos	☐ FALSO
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☑ VERDADERO
Se incluye la seguridad en equipos móviles	☐ FALSO

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	FALSO
Estan establecidas responsabilidades para controlar los cambios en equipos	VERDADERO
Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	VERDADERO
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	FALSO
Existe una separación de los entornos de desarrollo y producción	VERDADERO
Existen contratistas externos para la gestión de los Sistemas de Información	VERDADERO
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	FALSO
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	FALSO
Controles contra software maligno	VERDADERO
Realizar copias de backup de la información esencial para el negocio	VERDADERO
Existen logs para las actividades realizadas por los operadores y administradores	FALSO
Existen logs de los fallos detectados	VERDADERO
Existen rastro de auditoría	FALSO
Existe algún control en las redes	VERDADERO
Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	FALSO
Eliminación de los medios informáticos. Pueden disponer de información sensible	FALSO
Existe seguridad de la documentación de los Sistemas	FALSO
Existen acuerdos para intercambio de información y software	VERDADERO
Existen medidas de seguridad de los medios en el tránsito	FALSO
Existen medidas de seguridad en el comercio electrónico.	VERDADERO
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	VERDADERO
Existen medidas de seguridad en las transacciones en linea	VERDADERO
Se monitorean las actividades relacionadas a la seguridad	FALSO

CONTROL DE ACCESOS

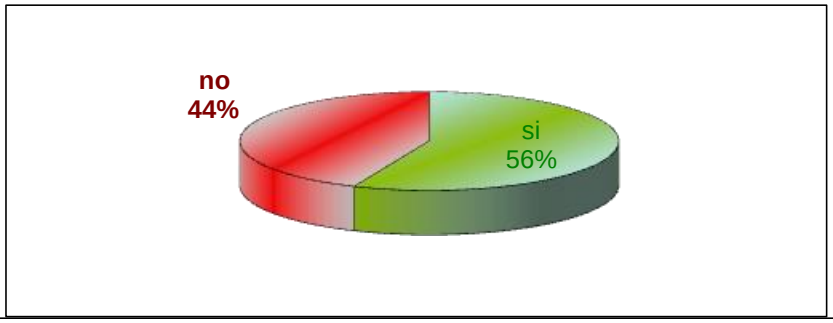
Existe una política de control de accesos	VERDADERO
Existe un procedimiento formal de registro y baja de accesos	FALSO
Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	VERDADERO
Existe una gestión de los password de usuarios	VERDADERO
Existe una revisión de los derechos de acceso de los usuarios	VERDADERO
Existe el uso del password	VERDADERO
Se protege el acceso de los equipos desatendidos	VERDADERO
Existen políticas de limpieza en el puesto de trabajo	FALSO
Existe una política de uso de los servicios de red	VERDADERO
Se asegura la ruta (path) desde el terminal al servicio	VERDADERO
Existe una autenticación de usuarios en conexiones externas	VERDADERO
Existe una autenticación de los nodos	VERDADERO
Existe un control de la conexión de redes	VERDADERO
Existe un control del routing de las redes	VERDADERO
Existe una identificación única de usuario y una automática de terminales	VERDADERO
Existen procedimientos de log-on al terminal	VERDADERO
Se ha incorporado medidas de seguridad a la computación móvil	FALSO
Está controlado el teletrabajo por la organización	FALSO

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Se asegura que la seguridad está implantada en los Sistemas de Información	FALSO
Existe seguridad en las aplicaciones	FALSO
Existen controles criptográficos.	VERDADERO
Existe seguridad en los ficheros de los sistemas	VERDADERO
Existe seguridad en los procesos de desarrollo, testing y soporte	VERDADERO
Existen controles de seguridad para los resultados de los sistemas	FALSO
Existe la gestión de los cambios en los SO.	FALSO
Se controlan las vulnerabilidades de los equipos	FALSO

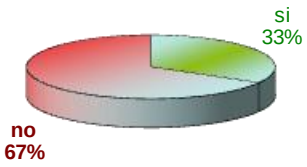
ADMINISTRACIÓN DE INCIDENTES	
Se comunican los eventos de seguridad	☑ VERDADERO
Se comunican los debilidades de seguridad	☐ FALSO
Existe definidas las responsabilidades ante de un incidente.	☐ FALSO
Existe un procedimiento formal de respuesta	☐ FALSO
Existe la gestión de incidentes	☐ FALSO
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Existen procesos para la gestión de la continuidad.	☐ FALSO
Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO
Existe un diseño, redacción e implantación de planes de continuidad	☐ FALSO
Existe un marco de planificación para la continuidad del negocio	☐ FALSO
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☐ FALSO
CUMPLIMIENTO	
Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☐ FALSO
Existe el resguardo de la propiedad intelectual	☑ VERDADERO
Existe el resguardo de los registros de la organización	☑ VERDADERO
Existe una revisión de la política de seguridad y de la conformidad técnica	☐ FALSO
Existen consideraciones sobre las auditorías de los sistemas	☐ FALSO

RESULTADOS AUTODIAGNÓSTICO GENERAL

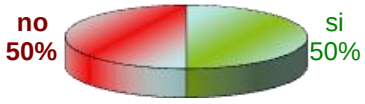


POR ÁREAS

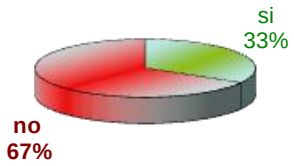
POLÍTICAS DE SEGURIDAD



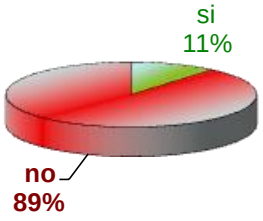
ORGANIZACIÓN DE LA SEGURIDAD



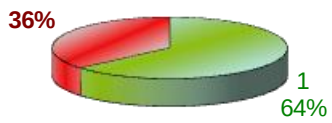
CLASIFICACIÓN Y CONTROL DE ACTIVOS



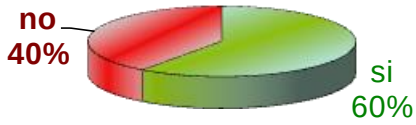
SEGURIDAD DEL PERSONAL



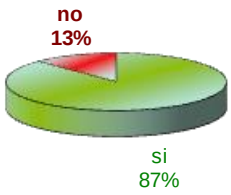
SEGURIDAD FÍSICA Y DEL ENTORNO



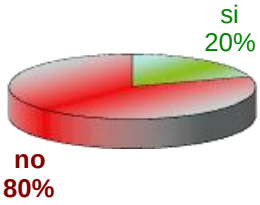
GESTIÓN DE COMUNICACIONES Y OPERACIONES



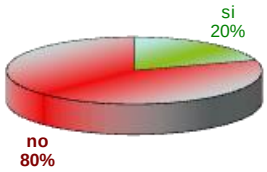
CONTROL DE ACCESOS



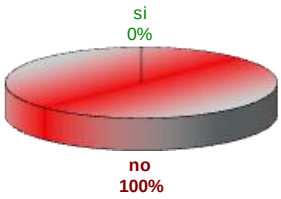
DESARROLLO Y MANTENIMIENTO DE SISTEMAS



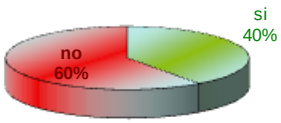
ADM. DE INCIDENTES



GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO



CONFORMIDAD



Anexo 6. Circular 052

La circular externa 052 de 2007, expedida por la Superintendencia Financiera de Colombia contiene los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios; se relaciona a continuación el cumplimiento por parte de Fullcarga Colombia respecto a la circular.

Circular 052		**Requisito**	**Requerido**	**% Cumplimiento**	**Observaciones**
2.1.4.	**Información confidencial**	La Clasificación de la información como confidencial deberá estar debidamente documentada y a disposición de la Superintendencia Financiera de Colombia.	SI	SI	Documento que defina la clasificación de la información según los criterios de la información que se definan por parte de la alta gerencia.
3.	**Obligaciones generales**	Incluir en sus políticas y procedimientos relativos a la administración de la información, los criterios de que tratan los numerales 2.1 y 2.2. (Criterios de seguridad y calidad de la información)	SI	NO	Implementar SGSI (ISO 27001)
3.1.	**Seguridad y calidad**	-	-	-	-

3.1.1.	**Seguridad y calidad**	Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.	SI	MEJORAR	Diagrama de red, diagrama de seguridad lógica, procedimientos de gestión de incidentes, soporte técnico.
3.1.2.	**Seguridad y calidad**	Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible.	SI	NO	Implementar SGSI (ISO 27001)
3.1.3.	**Seguridad y calidad**	Disponer que el envío de información a sus clientes, tales como certificaciones, extractos, notificaciones, sobreflex, entre otros, así como los medios (tarjetas débito y crédito, chequeras, etc.) se haga en condiciones de seguridad. Cuando la información que la entidad remite a sus clientes sea de carácter confidencial y se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.	NO	NO	Se deberá disponer de un correo cifrado para los correos de envío de información desde la plataforma. Definir política de prohibir enviar correo a clientes con información transaccional

3.1.4.	**seguridad y calidad**	Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad	SI	MEJORAR	Implementar políticas de manejo de la información de los clientes. Bloquear completamente los dispositivos de salida de los PC en la oficina.
3.1.5.	**Seguridad y calidad**	Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad	SI	MEJORAR	Implementar políticas de manejo de la información de los clientes. Bloquear completamente los dispositivos de salida de los PC en la oficina.
3.1.6.	**seguridad y calidad**	Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.	SI	MEJORAR	Política de manejo de contraseñas (políticas de seguridad)
3.1.7.	**seguridad y calidad**	Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.	SI	MEJORAR	Implementar políticas de manejo de la información de los clientes. Bloquear completamente los dispositivos de salida de los PC en la oficina.

3.1.8.	**Seguridad y calidad**	Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.	SI	NO	Implementar auditorías a los controles de seguridad (ISO 27001)

3.1.9.	**Seguridad y calidad**	Disponer de los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales se les prestará servicios por los diferentes canales, dejando constancia de ello. En desarrollo de lo anterior, la entidad deberá permitir que el cliente, por lo menos, inscriba las cuentas a las cuales realizará transferencias o pagos, defina montos, número de operaciones y canales. En cualquier caso, los montos máximos deberán ser definidos por la entidad. Así mismo, deberá permitir que el cliente registre las direcciones IP, los números de los teléfonos fijos y móviles desde los cuales operará. La entidad podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.	SI	SI	*Logs* de plataforma - Herramienta de gestión de usuarios de TITAN y SIGMA, gestión de usuarios en POS

3.1.10.	**Seguridad y calidad**	Ofrecer, cuando el cliente así lo exija, la posibilidad de manejar una contraseña diferente para cada uno de los canales.	SI	SI	Contraseña por medio de venta. Para SMS no aplicaría.
3.1.11.	**Seguridad y calidad**	Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.	SI	MEJORAR	Procedimiento de administración de servidores, Instructivo de carga de software en POS. Palabra PASO, claves para actualización o cambio de software.
3.1.12.	**Seguridad y calidad**	Establecer procedimientos para el bloqueo de canales o de medios, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.	SI	SI	Herramientas de bloqueo de cliente, POS, usuario por SIGMA, bloqueo por número de intentos, bloqueo de tarjeta de coordenadas, documentación para desbloquear usuarios, POS, Clientes y evidencia de estas actividades registradas en los log.

3.1.13.	**Seguridad y calidad**	Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación de las operaciones que no correspondan a sus hábitos.	N/A	N/A	N/A
3.1.14.	**Seguridad y calidad**	Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales y medios de servicio al cliente y al usuario. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.	SI	MEJORAR	Políticas de seguridad, procedimientos de entrega de dispositivos al cliente.
3.1.15.	**Seguridad y calidad**	Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.	SI	NO	Definir procedimiento para reaccionar ante evidencia de la alteración de los POS

3.1.16.	**Seguridad y calidad**	Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.	SI	MEJORAR	Se tienen sincronización de los servidores contra un servidor NTP externo, no contra el proporcionado por la superintendencia (horalegal.sic.gov.co)
3.1.17.	**Seguridad y calidad**	Tener en operación solo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.	SI	MEJORAR	Procedimientos de mantenimiento de software y hardware, hoja de vida de equipos.
3.1.18.	**Seguridad y calidad**	Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.	SI	SI	Alarmas GW, Nagios, MRTG Telmex.
3.1.19.	**Seguridad y calidad**	Incluir en el informe de gestión a que se refiere el artículo 47 de la ley 222 de 1995 y sus modificaciones, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.	SI	SI	El informe de gestión deberá contener una exposición fiel sobre la evolución de los negocios y la situación jurídica, económica y administrativa de la sociedad.

3.1.20.	**seguridad y calidad**	Considerar en sus políticas y procedimiento relativos a los canales y medios de distribución de productos y servicios, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.	SI	NA	NA
3.2.	**Tercerización**	-	-	-	-
3.2.1.	**Tercerización**	Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.	SI	MEJORAR	Actualizar procedimiento de adquisición de servicios por tercerización para temas relacionados con la plataforma.

3.2.2.	**Tercerización**	Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente capítulo, por lo menos, los siguientes aspectos: a) Niveles de servicio y operación. b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas. c) Propiedad de la información. d) Restricciones sobre el software empleado. e) Normas de seguridad informática y física a ser aplicadas. f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información. g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.	SI	MEJORAR	Revisar todos los proveedores de servicios para la plataforma que cumplan con los requerimientos, en especial f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información y g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

3.2.3.	**Tercerización**	Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas	SI	MEJORAR	Solicitar actualización a TELMEX y Getronics de estos planes.
3.2.4.	**Tercerización**	Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados.	SI	SI	Carnet empresarial y acceso a las instalaciones por medio de lector biométrico. Para el caso de *datacenter*, se exige tarjeta de proximidad y autorización vía correo electrónico previa a la visita.
3.2.5.	**Tercerización**	Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados	SI	SI	Implementación de VPN con cifrado AES y 3DES
3.3.	**Documentación**	-	-	-	-

3.3.1.	**Documentación**	Dejar constancia de todas las operaciones que se realicen a través de los distintos canales de distribución de servicios para clientes y usuarios que contenga por lo menos lo siguiente: fecha, hora, código del equipo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión) número de la operación, cuenta(s), costo de la misma para el usuario.	SI	SI	*Logs* de plataforma - Tabla de registros de accesos a la plataforma.
3.3.2.	**Documentación**	Velar por que los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las normas vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los diferentes canales de distribución.	SI	NO	Auditoría

3.3.3.	**Documentación**	Mantener a disposición de la SFC estadísticas anuales con corte a 31 de diciembre de cada año respecto de la prestación de servicios a través de cada uno de los canales de distribución, que contemplen: el número de operaciones realizadas y el nivel de disponibilidad del canal. Esta información deberá ser conservada por un término de tres (3) años.	SI	MEJORAR	Implementación de un reporte según se indica en la circular externa 014 de 2008
3.3.4.	**Documentación**	Cuando a través de los distintos canales se pidan y se realicen donaciones, se deberá generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.	SI	MEJORAR	Generar política de no realizar donaciones por ningún POS.

3.3.5.	**Documentación**	Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.	SI	SI	Gestión de la documentación de los clientes

3.3.6.	**Documentación**	Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.	SI	NO	Crear log de consulta de información desde SIGMA y TITAN.
3.3.7.	**Documentación**	Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.	SI	SI	Procesos de entrega por parte de los POS en logística.

3.3.8.	**Documentación**	Dejar constancia del cumplimiento de la obligación establecida en el numeral 3.4.4.	SI	SI	Proceso de entrega de POS a un cliente, firma de aceptación y conocimiento del manejo de la herramienta. Aceptación al ingresar por primera vez a TITAN.
3.3.9.	**Documentación**	Grabar las llamadas realizadas por los clientes a los centros de atención telefónica que conlleven a la consulta o actualización de su información	SI	SI	Servicio ofrecido por el *Call Center*, se graba el 100% de las llamadas.
3.3.10.	**Documentación**	La información a que se refieren los numeral 3.3.1, 3.3.6 y 3.3.9 deberá ser conservada por lo menos por dos (2) años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.	SI	MEJORAR	Depende de implementar la 3.6 para cumplir este numeral.
3.4.	**Divulgación de información**	-	-	-	-

3.4. 1.	**Divulgación de información**	En concordancia con lo dispuesto en el artículo 97 del E.O.S.F., suministrar a los clientes información clara, completa y oportuna de los productos, servicios y operaciones	SI	SI	Página corporativa, herramientas para la gestión productos y de menús
3.4. 2.	**Divulgación de Información**	Dar a conocer a sus clientes y usuarios, por el respectivo canal y en forma previa a la realización de la operación, el costo de la misma, si lo hay, brindándoles la posibilidad de efectuarla o no. Tratándose de cajeros automáticos la obligación solo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia	SI	SI	Confirmación de los parámetros de la operación a realizar.
3.4. 3.	**Divulgación de Información**	Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.	N/A	N/A	N/A

3.4. 4.	**Divulgación de Información**	Informar y capacitar a los clientes acerca de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos	SI	SI	Procedimientos y documentos del tema
3.4. 5.	**Divulgación de Información**	Establecer y publicar por los canales de distribución, en los que sea posible, las medidas de seguridad que deberá adoptar el cliente para el uso de los mismos	SI	SI	Portal corporativo, boletines de seguridad, etc.
3.4. 6.	**Divulgación de Información**	Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales	SI	MEJORAR	Crear un manual de seguridad para el usuario de los productos.

3.4. 7.	**Divulgación de Información**	Expedir un soporte, en papel o por medios electrónicos, al momento de la realización de cada transacción. Dicho soporte deberá contener al menos la siguiente información: fecha, hora (hora y minuto), código del equipo (para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles: el número desde el cual se hizo la conexión), número, costo de la operación para el cliente o usuario, tipo, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan la operación. Se deberán ocultar los números de las cuentas con excepción de los últimos cuatro (4) caracteres, salvo cuando se trate de la cuenta que recibe una transferencia. Cuando no se pueda entregar el soporte, se deberá advertir previamente al cliente o usuario de esta situación. Para el caso de IVR se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la transacción. En relación con el costo de la operación y tratándose de cajeros automáticos la obligación solo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia.	SI	MEJORAR	

3.4. 8.	**Divulgación de Información**	Entregar constancia, dentro del procedimiento de cancelación solicitado por el cliente, de un producto, en la que se advierta encontrarse a paz y salvo por todo concepto, asegurándose que los futuros reportes a las centrales de riesgo sean consistentes con su estado de cuenta. Tratándose de tarjetas de crédito dicha constancia deberá entregarse al cliente en un tiempo máximo de cuarenta y cinco (45) días, contados a partir de la fecha de solicitud de la cancelación.	N/A	N/A	Se maneja la operación 100% prepago.
4	**Obligaciones Adicionales por Tipo de Canal**	-	-	-	-
4.1.	**Oficinas**	-	N/A	N/A	N/A
4.2.	**Cajeros Automáticos (ATM)**	-	N/A	N/A	N/A
4.3.	**Receptores de Cheques**	-	N/A	N/A	N/A
4.4.	**Receptores de Dinero en Efectivo**	-	N/A	N/A	Aplicaría para las *vending*, pero estas no entrarían a operar con el tema de CNB. Por lo que se excluyen.

4.5.	**POS (incluye PIN Pad)**	-	-	-	-
4.5.1.	**POS (incluye PIN Pad)**	La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad.	SI	SI	Los POS soportan y consideran la seguridad requerida, pero toca implementar la aplicación de nuestra parte.
4.5.2.	**POS (incluye PIN Pad)**	Cumplir el estándar EMV (estándar de interoperabilidad de tarjetas con chip y TPV o datáfonos, para la autentificación de pagos a través de tarjetas de crédito y débito - Europay, MasterCard, VISA).	SI	MEJORAR	Los POS soportan el estándar, pero toca implementar la aplicación de nuestra parte.
4.5.3.	**POS (incluye PIN Pad)**	Los administradores de las redes de este canal deberán validar automáticamente la autenticidad del datáfono que se intenta conectar a ellos, así como el medio de comunicación a través del cual operará.	SI	SI	Identificación por medio de número de serie y el canal está dado por APN privado.
4.5.4.	**POS (incluye PIN Pad)**	Establecer procedimientos que le permitan a los responsables de los datáfonos en los establecimientos comerciales, confirmar la identidad de los funcionarios autorizados para retirar o hacerle mantenimiento a los equipos.	SI	NO	Definir el procedimiento solicitado

4.5.5.	**POS (incluye PIN Pad)**	Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados.	SI	SI	Los POS seleccionados cumplirán con la condición.
4.5.6.	**POS (incluye PIN Pad)**	Contar con mecanismos que reduzcan la posibilidad de que terceros puedan ver la clave digitada por el cliente o usuario.	SI	SI	Al ingresar la clave esta queda enmascarada para evitar sea vista por terceros en todos los POS.
4.6.	**Sistemas de Audio Respuesta (IVR)**	-	-	-	-
4.6.1.	**Sistemas de Audio Respuesta (IVR)**	Permitir al cliente confirmar la información suministrada en la realización de la transacción.	SI	SI	Se solicita confirmación en cada TRX. Aunque no será un medio a usar para CNB
4.6.2.	**Sistemas de Audio Respuesta (IVR)**	Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público	SI	NO	Es un sistema autónomo y de igual manera no aplica este medio para CNB
4.7.	**Centro de Atención Telefónica (Call Center, Contact Center)**	-	N/A	N/A	No se realizaran operaciones por este canal - NO Aplica

4.8.	**Sistemas de Acceso Remoto para Clientes**	Las entidades que ofrezcan servicio de acceso remoto para la realización de transacciones deberán contar con un módulo de seguridad de hardware para el sistema, que cumpla al menos con el estándar de seguridad FIPS-140-2 (*Federal Information Processing Standard*), el cual deberá ser de propósito específico (*appliance*) totalmente separado e independiente de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de *gateways*, de servidores de acceso remoto (RAS) y/o de concentradores.	NO	NO	El sistema de seguridad cumple el estándar, pero no la independencia física, si se opta por tener puntos RAS se deberá contemplar comprar otro FW.
4.9.	**Internet**	-	-	-	-
4.9.1.	**Internet**	Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.	SI	SI	Portal HTPS - certificado de servidor seguro *VeriSing*

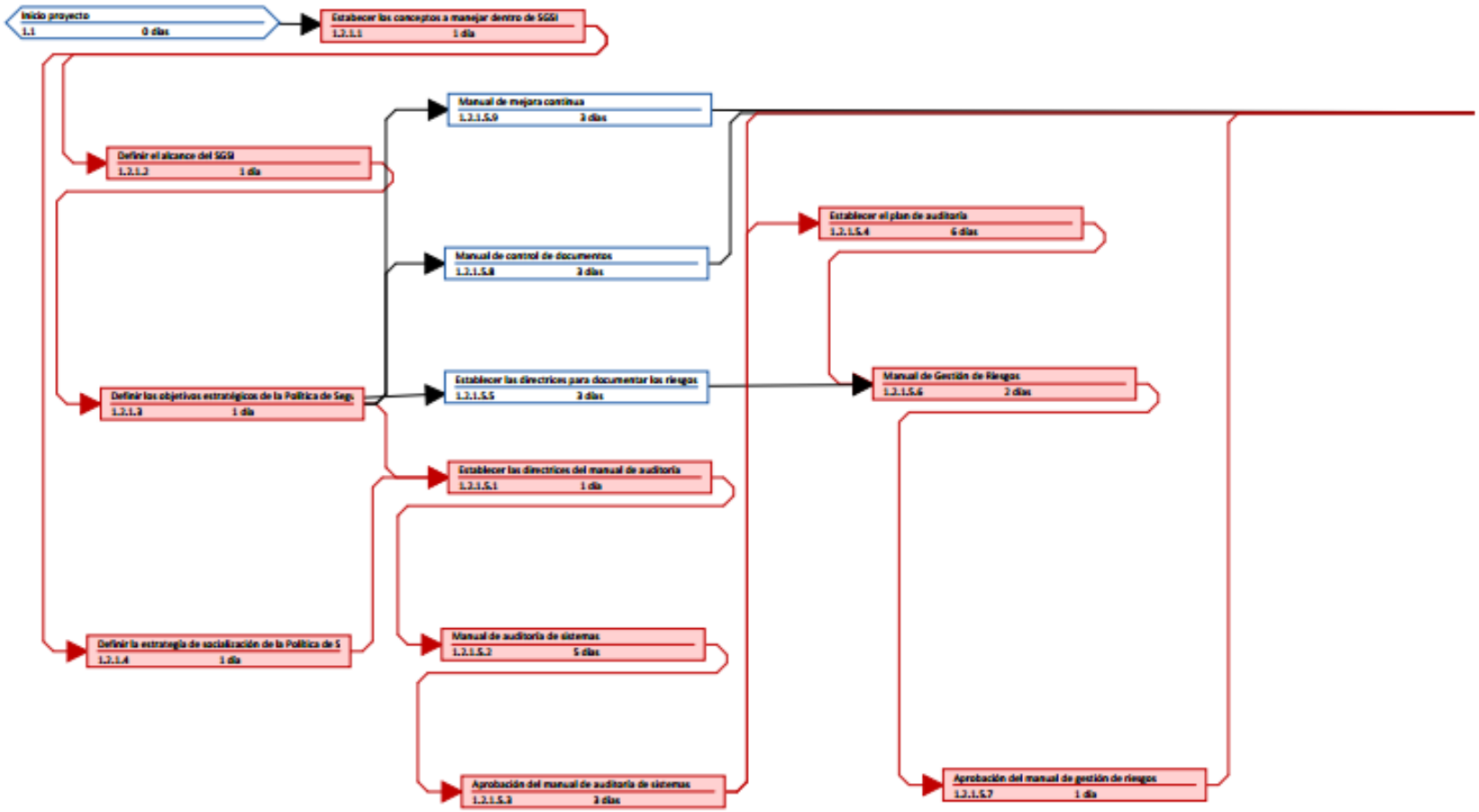
4.9.2.	**Internet**	Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.	SI	NO	
4.9.3.	**Internet**	Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.	SI	SI	Teclado virtual, tarjeta de coordenadas.
4.9.4.	**Internet**	Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.	SI	SI	Definido en 30 minutos
4.9.5.	**Internet**	Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.	SI	NO	Se resguarda la información, por lo que estaría pendiente esta sea visualizada.

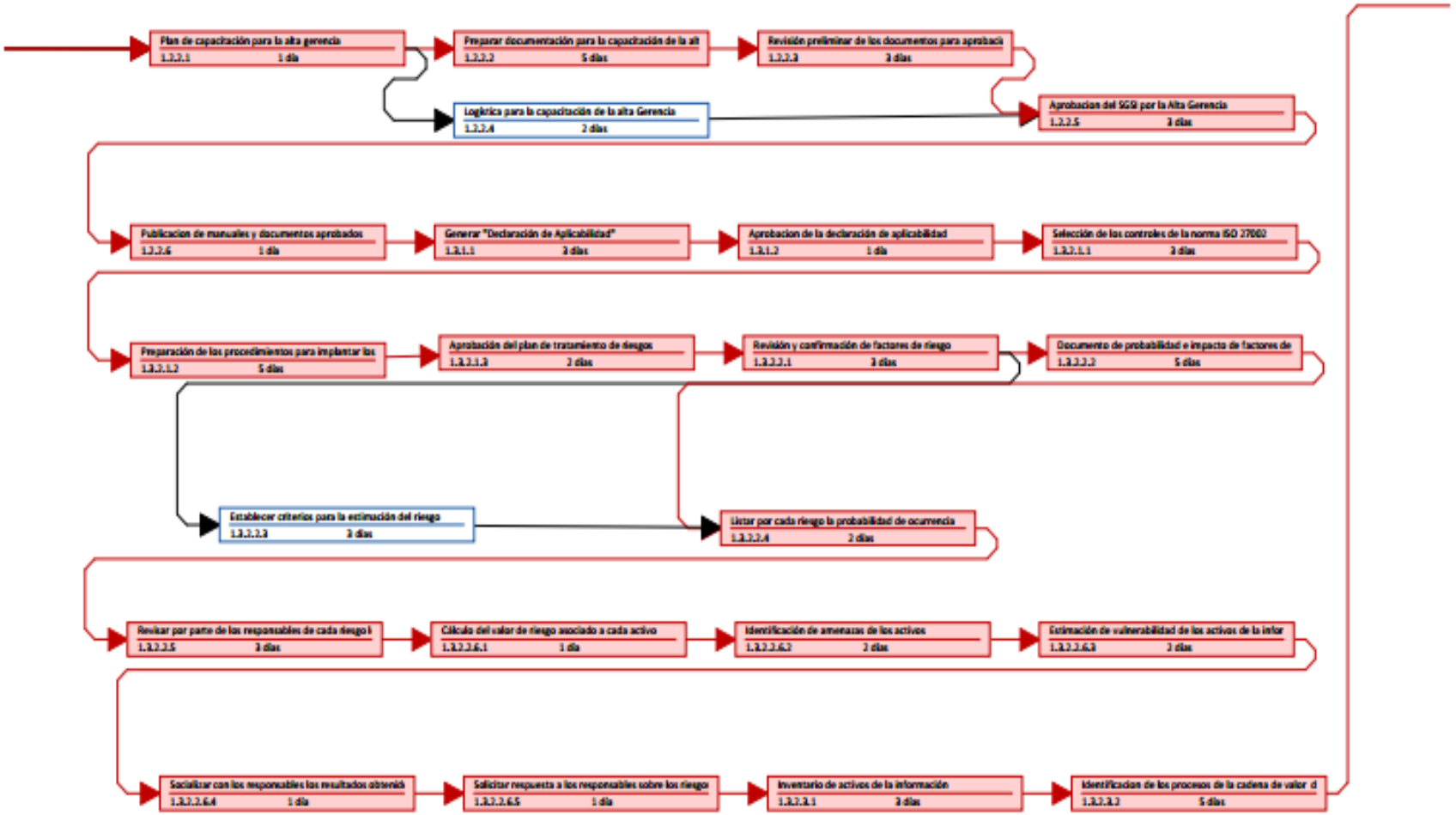
4.9.6.	**Internet**	Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (*link*) de su sitio *web*, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.	SI	SI	Manejo del dominio .co, boletines de seguridad notificando esto.
4.10.	**Prestación de Servicios a través de Nuevos Canales**	-	N/A	N/A	
5.	**Reglas sobre Actualización de Software**	-	-	-	-
5.1.	**Reglas sobre Actualización de Software**	Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.	SI	SI	Se mantiene independencia física y lógica de los tres ambientes.
5.2.	**Reglas sobre Actualización de Software**	Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.	SI	MEJORAR	Se gestiona las versiones pero falta oficializar el procedimiento.

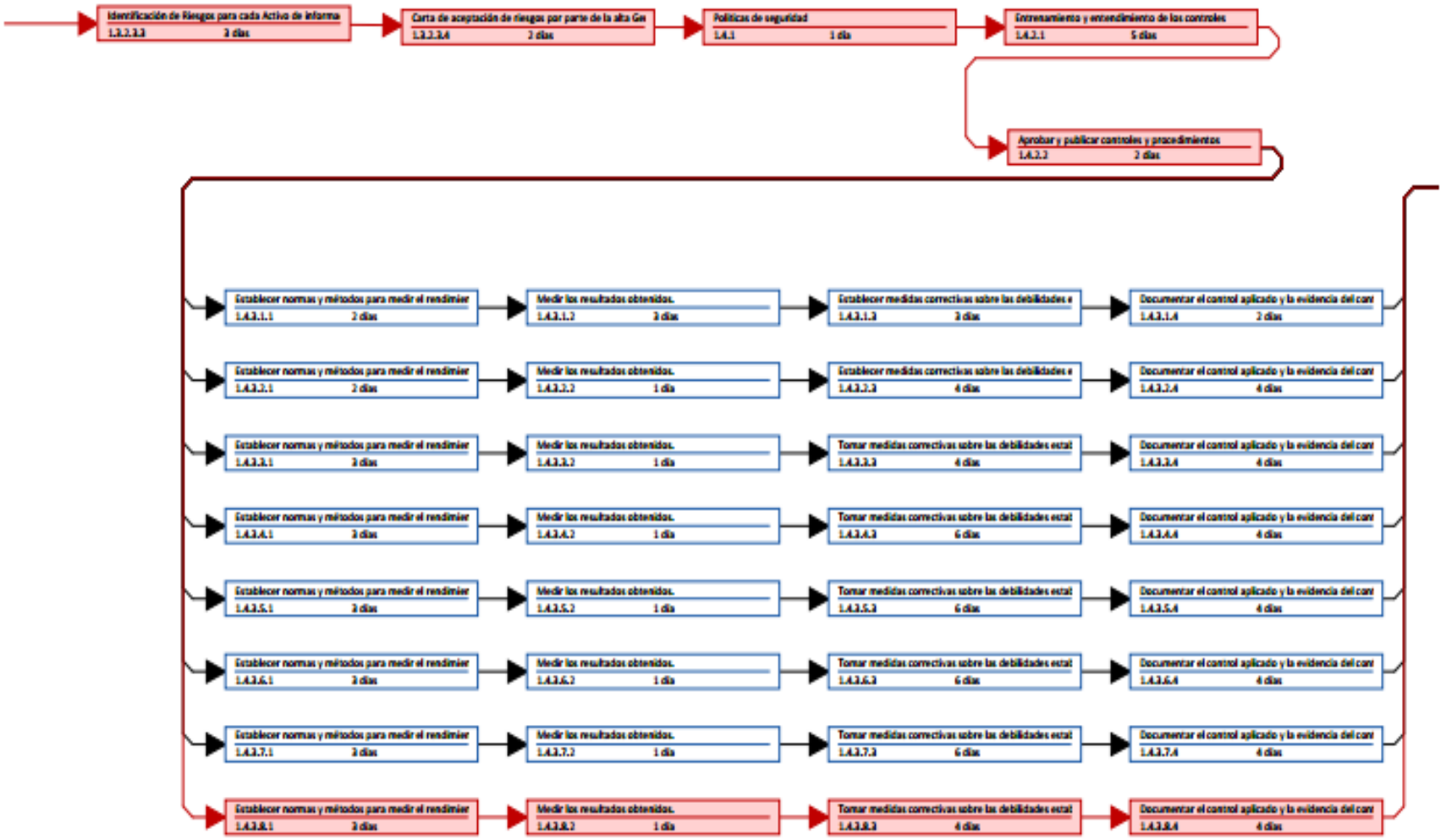
5.3.	**Reglas sobre Actualización de Software**	Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.	SI	SI	Como política principal no se maneja datos de clientes para la realización de pruebas.
5.4.	**Reglas sobre Actualización de Software**	Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.	SI	MEJORAR	Se tiene definido un procedimiento para tal fin, pero falta oficializar y normalizar.
5.5.	**Reglas sobre Actualización de Software**	Contar con interfaces para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.	SI	SI	Toda herramienta tiene como base la autogestión.
5.6.	**Reglas sobre Actualización de Software**	Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software	SI	NO	Se tiene la información pero no se encuentra compilada en un único punto.

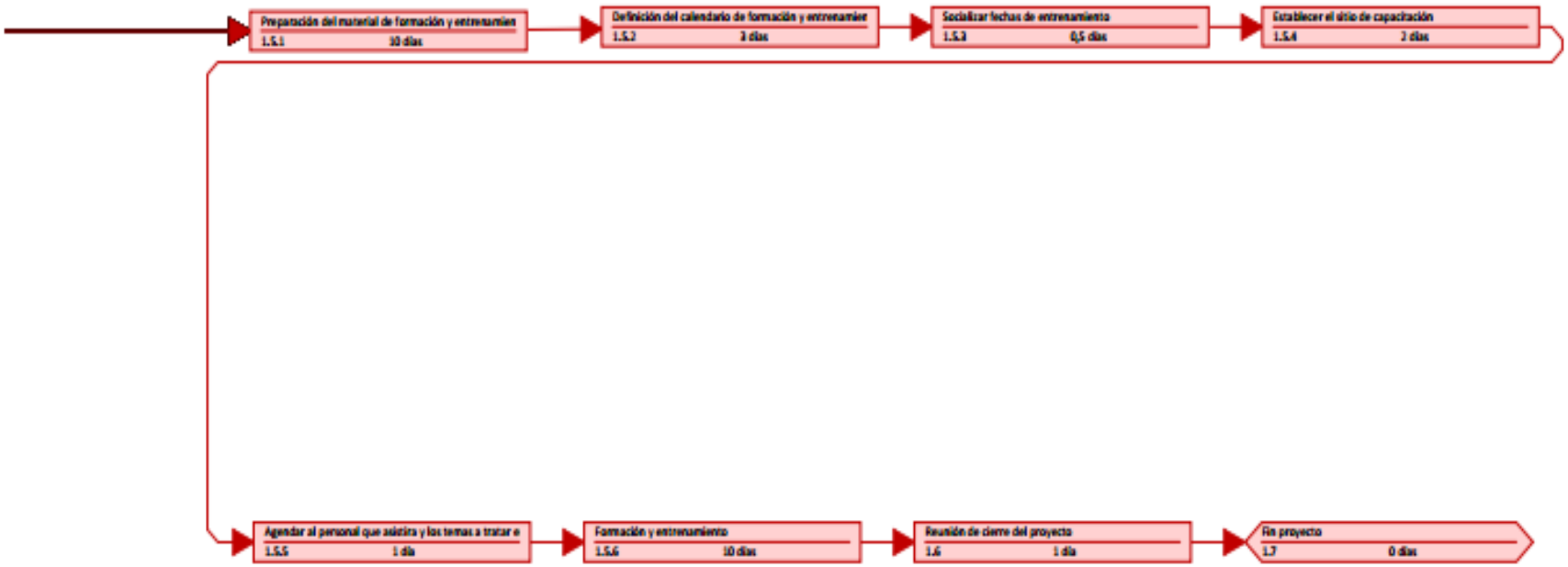
6.	**Obligaciones Específicas por Tipo de Medio – Tarjetas débito y crédito**		NO	N/A	N/A
7.	**Análisis de Vulnerabilidades**	-	NO	N/A	N/A

Anexo 7. Diagrama de red



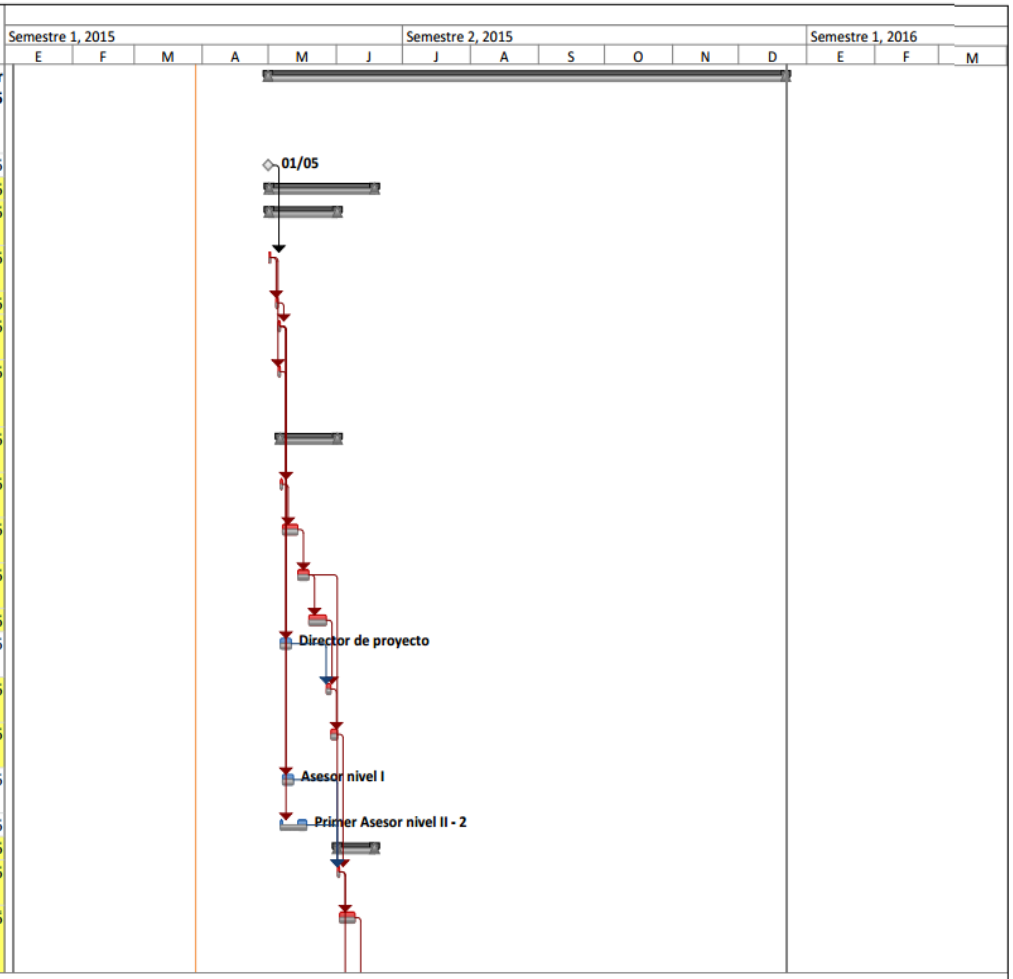

Plan de capacitación para la alta gerencia
1.2.2.1 1 día
Preparar documentación para la capacitación de la alt
1.2.2.2 5 días
Revisión preliminar de los documentos para aprobació
1.2.2.3 3 días
Logística para la capacitación de la alta Gerencia
1.2.2.4 2 días
Aprobacion del SGSI por la Alta Gerencia
1.2.2.5 3 días
Publicacion de manuales y documentos aprobados
1.2.2.6 1 día
Generar "Declaración de Aplicabilidad"
1.3.1.1 3 días
Aprobacion de la declaración de aplicabilidad
1.3.1.2 1 día
Selección de los controles de la norma ISO 27002
1.3.2.1.1 3 días
Preparación de los procedimientos para implantar los
1.3.2.1.2 5 días
Aprobación del plan de tratamiento de riesgos
1.3.2.1.3 2 días
Revisión y confirmación de factores de riesgo
1.3.3.3.1 3 días
Documento de probabilidad e impacto de factores de
1.3.3.3.2 5 días
Establecer criterios para la estimación del riesgo
1.3.3.3.3 3 días
Listar por cada riesgo la probabilidad de ocurrencia
1.3.3.3.4 2 días
Revisar por parte de los responsables de cada riesgo l
1.3.3.3.5 3 días
Cálculo del valor de riesgo asociado a cada activo
1.3.3.3.6.1 1 día
Identificación de amenazas de los activos
1.3.3.3.6.2 2 días
Estimación de vulnerabilidad de los activos de la infor
1.3.3.3.6.3 2 días
Socializar con los responsables los resultados obtenid
1.3.3.3.6.4 1 día
Solicitar respuesta a los responsables sobre los riesgo
1.3.3.3.6.5 1 día
Inventario de activos de la información
1.3.3.3.3.1 3 días
Identificacion de los procesos de la cadena de valor d
1.3.3.3.3.2 5 días


Identificación de Riesgos para cada Activo de informa
1.3.2.3.3 3 días
Carta de aceptación de riesgos por parte de la alta Ge
1.3.2.3.4 2 días
Políticas de seguridad
1.4.1 1 día
Entrenamiento y entendimiento de los controles
1.4.2.1 5 días
Aprobar y publicar controles y procedimientos
1.4.2.2 2 días
Establecer normas y métodos para medir el rendimier
1.4.3.1.1 2 días
Medir los resultados obtenidos.
1.4.3.1.2 3 días
Establecer medidas correctivas sobre las debilidades e
1.4.3.1.3 3 días
Documentar el control aplicado y la evidencia del cont
1.4.3.1.4 2 días
Establecer normas y métodos para medir el rendimier
1.4.3.2.1 2 días
Medir los resultados obtenidos.
1.4.3.2.2 1 día
Establecer medidas correctivas sobre las debilidades e
1.4.3.2.3 4 días
Documentar el control aplicado y la evidencia del cont
1.4.3.2.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.3.1 3 días
Medir los resultados obtenidos.
1.4.3.3.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.3.3 4 días
Documentar el control aplicado y la evidencia del cont
1.4.3.3.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.4.1 3 días
Medir los resultados obtenidos.
1.4.3.4.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.4.3 6 días
Documentar el control aplicado y la evidencia del cont
1.4.3.4.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.5.1 3 días
Medir los resultados obtenidos.
1.4.3.5.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.5.3 6 días
Documentar el control aplicado y la evidencia del cont
1.4.3.5.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.6.1 3 días
Medir los resultados obtenidos.
1.4.3.6.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.6.3 6 días
Documentar el control aplicado y la evidencia del cont
1.4.3.6.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.7.1 3 días
Medir los resultados obtenidos.
1.4.3.7.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.7.3 6 días
Documentar el control aplicado y la evidencia del cont
1.4.3.7.4 4 días
Establecer normas y métodos para medir el rendimier
1.4.3.8.1 3 días
Medir los resultados obtenidos.
1.4.3.8.2 1 día
Tomar medidas correctivas sobre las debilidades exist
1.4.3.8.3 4 días
Documentar el control aplicado y la evidencia del cont
1.4.3.8.4 4 días

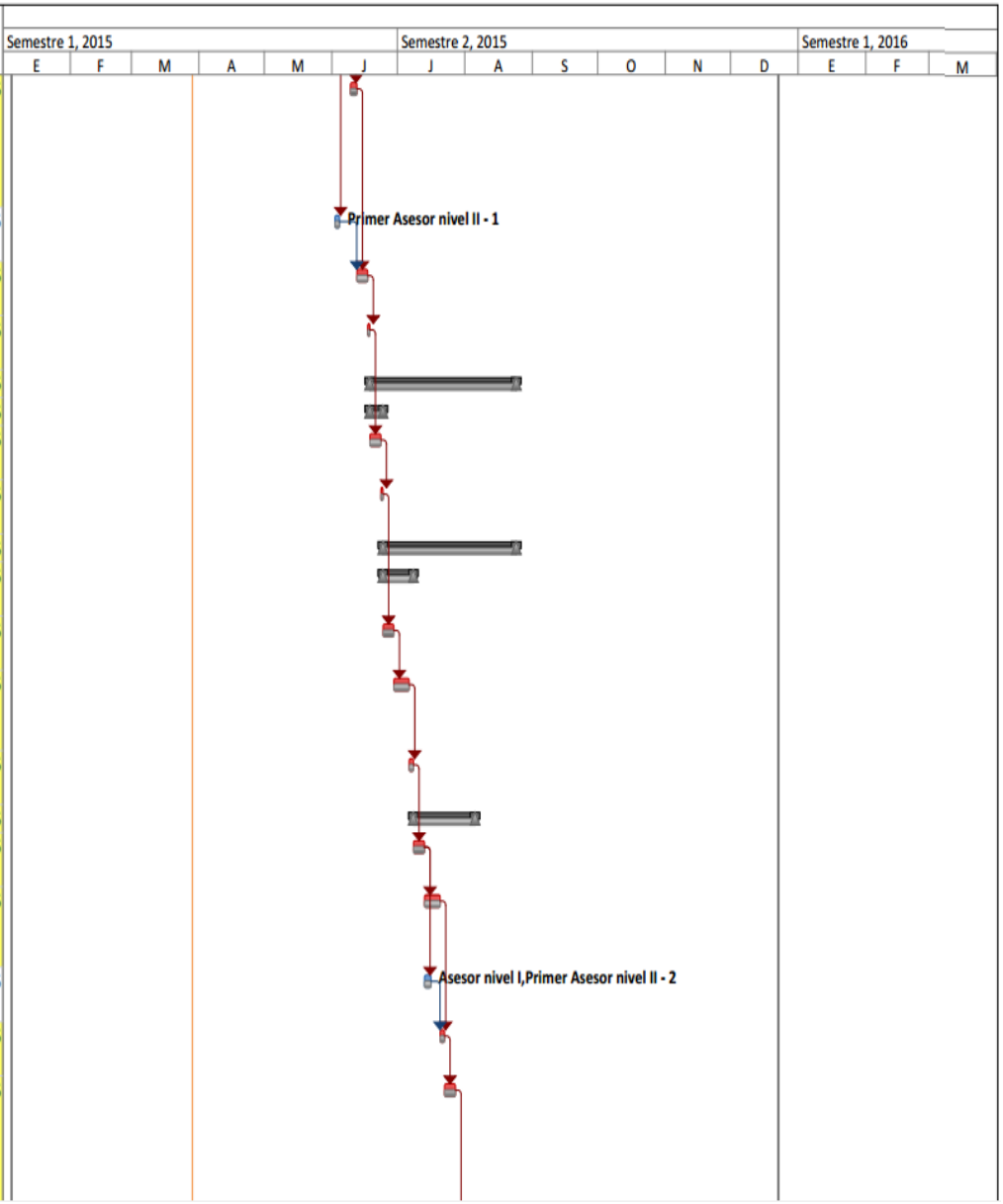

Preparación del material de formación y entrenamien
1.5.1 10 días
Definición del calendario de formación y entrenamier
1.5.2 3 días
Socializar fechas de entrenamiento
1.5.3 0,5 días
Establecer el sitio de capacitación
1.5.4 2 días
Agendar al personal que asistirá y los temas a tratar e
1.5.5 1 día
Formación y entrenamiento
1.5.6 10 días
Reunión de cierre del proyecto
1.6 1 día
Fin proyecto
1.7 0 días

Anexo 8. Diagrama de Gant

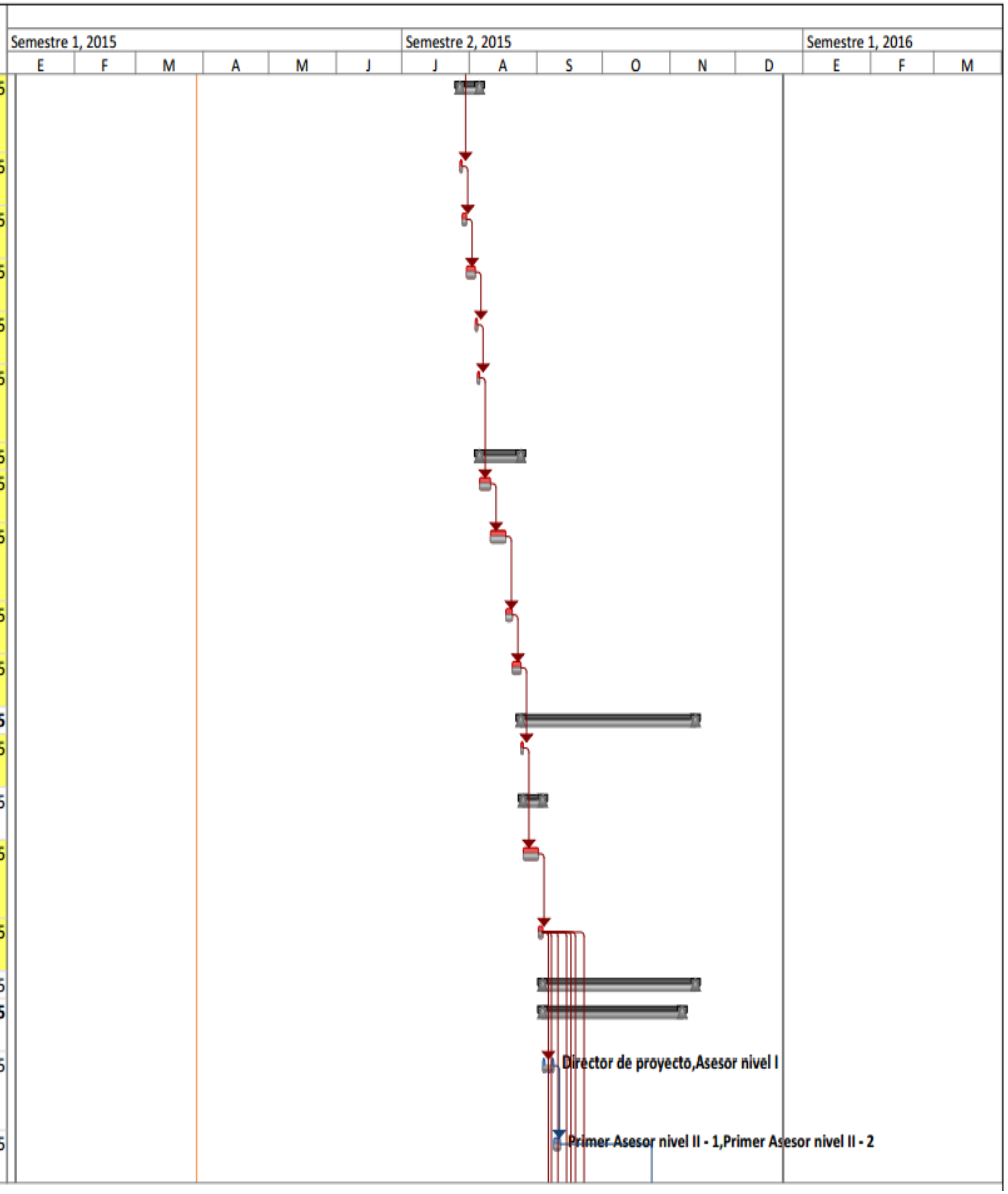
Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
1		**1**	**0%**	**Implementación Sistema de Gestión de Seguridad de la Información para el proceso de recarga electrónica en Fullcarga Colombia**	**vie 01/05/15**	**mar 22/12/15**
2		1.1	10...	Inicio proyecto	vie 01/05/15	vie 01/05/15
3		1.2	0%	Diseño del SGSI	vie 01/05/15	jue 18/06/15
4		1.2.1	0%	Definicion de fundamentos del SGSI	vie 01/05/15	lun 01/06/15
5		1.2.1.1	0%	Estabecer los conceptos a manejar dentro de SGSI	vie 01/05/15	vie 01/05/15
6		1.2.1.2	0%	Definir el alcance del SGSI	lun 04/05/15	mar 05/05/15
7		1.2.1.3	0%	Definir los objetivos estratégicos de la Política de	mar 05/05/15	mié 06/05/15
8		1.2.1.4	0%	Definir la estrategía de socialización de la Política de Seguridad	mar 05/05/15	mié 06/05/15
9		1.2.1.5	0%	Manual de Gestión de Seguridad de la Información	mié 06/05/15	lun 01/06/15
10		1.2.1.5.1	0%	Establecer las directrices del manual de auditoría	mié 06/05/15	jue 07/05/15
11		1.2.1.5.2	0%	Manual de auditoría de sistemas	jue 07/05/15	jue 14/05/15
12		1.2.1.5.3	0%	Aprobación del manual de auditoría de sistemas	jue 14/05/15	mar 19/05/15
13		1.2.1.5.4	0%	Establecer el plan de auditorí	mar 19/05/15	mié 27/05/15
14		1.2.1.5.5	0%	Establecer las directrices para documentar los riesgos	mié 06/05/15	lun 11/05/15
15		1.2.1.5.6	0%	Manual de Gestión de Riesgos	mié 27/05/15	vie 29/05/15
16		1.2.1.5.7	0%	Aprobación del manual de gestión de riesgos	vie 29/05/15	lun 01/06/15
17		1.2.1.5.8	0%	Manual de control de documentos	jue 07/05/15	mar 12/05/15
18		1.2.1.5.9	0%	Manual de mejora continua	mié 06/05/15	lun 18/05/15
19		1.2.2	0%	Definición del SGSI	lun 01/06/15	jue 18/06/15
20		1.2.2.1	0%	Plan de capacitación para la alta gerencia	lun 01/06/15	mar 02/06/15
21		1.2.2.2	0%	Preparar documentación para la capacitación de la alta gerencia	mar 02/06/15	mar 09/06/15



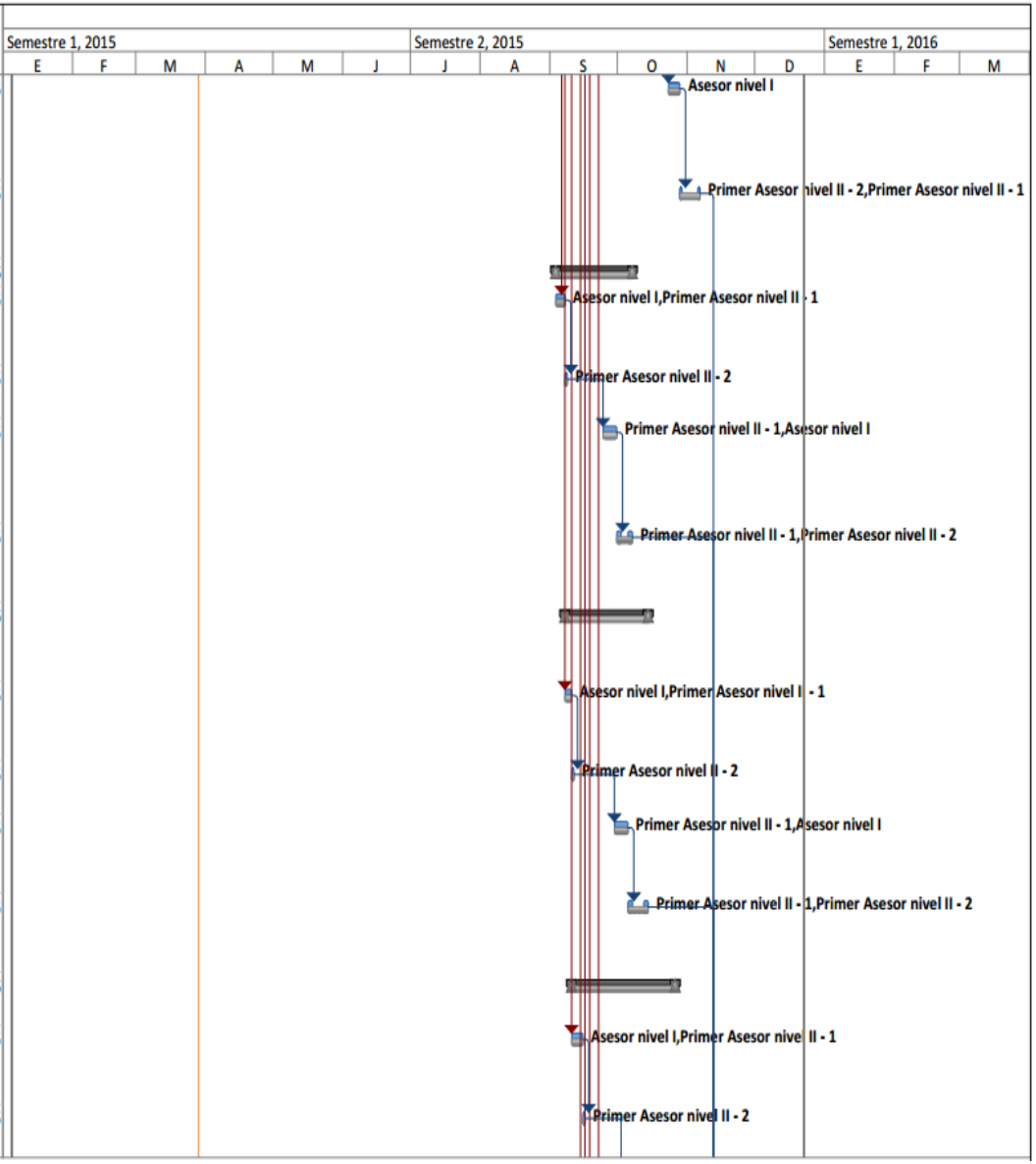
Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
22		1.2.2.3	0%	Revisión preliminar de los documentos para aprobación por los gestores del proceso de administración de la calidad	mar 09/06/15	vie 12/06/15
23		1.2.2.4	0%	Logística para la capacitación de la alta Gerencia	mar 02/06/15	jue 04/06/15
24		1.2.2.5	0%	Aprobacion del SGSI por la Alta Gerencia	vie 12/06/15	mié 17/06/15
25		1.2.2.6	0%	Publicacion de manuales y documentos aprobados	mié 17/06/15	jue 18/06/15
26		1.3	0%	Diagnóstico del SGSI	jue 18/06/15	lun 24/08/15
27		1.3.1	0%	Carta de aplicabilidad	jue 18/06/15	mié 24/06/15
28		1.3.1.1	0%	Generar "Declaración de Aplicabilidad"	jue 18/06/15	mar 23/06/15
29		1.3.1.2	0%	Aprobacion de la declaración de aplicabilidad	mar 23/06/15	mié 24/06/15
30		1.3.2	0%	Análisis de riesgos	mié 24/06/15	lun 24/08/15
31		1.3.2.1	0%	Plan de tratamiento de riesgos	mié 24/06/15	mié 08/07/15
32		1.3.2.1.1	0%	Selección de los controles de la norma ISO 27002	mié 24/06/15	lun 29/06/15
33		1.3.2.1.2	0%	Preparación de los procedimientos para implantar los controles	lun 29/06/15	lun 06/07/15
34		1.3.2.1.3	0%	Aprobación del plan de tratamiento de riesgos	lun 06/07/15	mié 08/07/15
35		1.3.2.2	0%	Estimación de Riesgos	mié 08/07/15	mié 05/08/15
36		1.3.2.2.1	0%	Revisión y confirmación de factores de riesgo	mié 08/07/15	lun 13/07/15
37		1.3.2.2.2	0%	Documento de probabilidad e impacto de factores de riesgo	lun 13/07/15	lun 20/07/15
38		1.3.2.2.3	0%	Establecer criterios para la estimación del riesgo	lun 13/07/15	jue 16/07/15
39		1.3.2.2.4	0%	Listar por cada riesgo la probabilidad de ocurrencia	lun 20/07/15	mié 22/07/15
40		1.3.2.2.5	0%	Revisar por parte de los responsables de cada riesgo los criterios y definición establecido a cada riesgo.	mié 22/07/15	lun 27/07/15



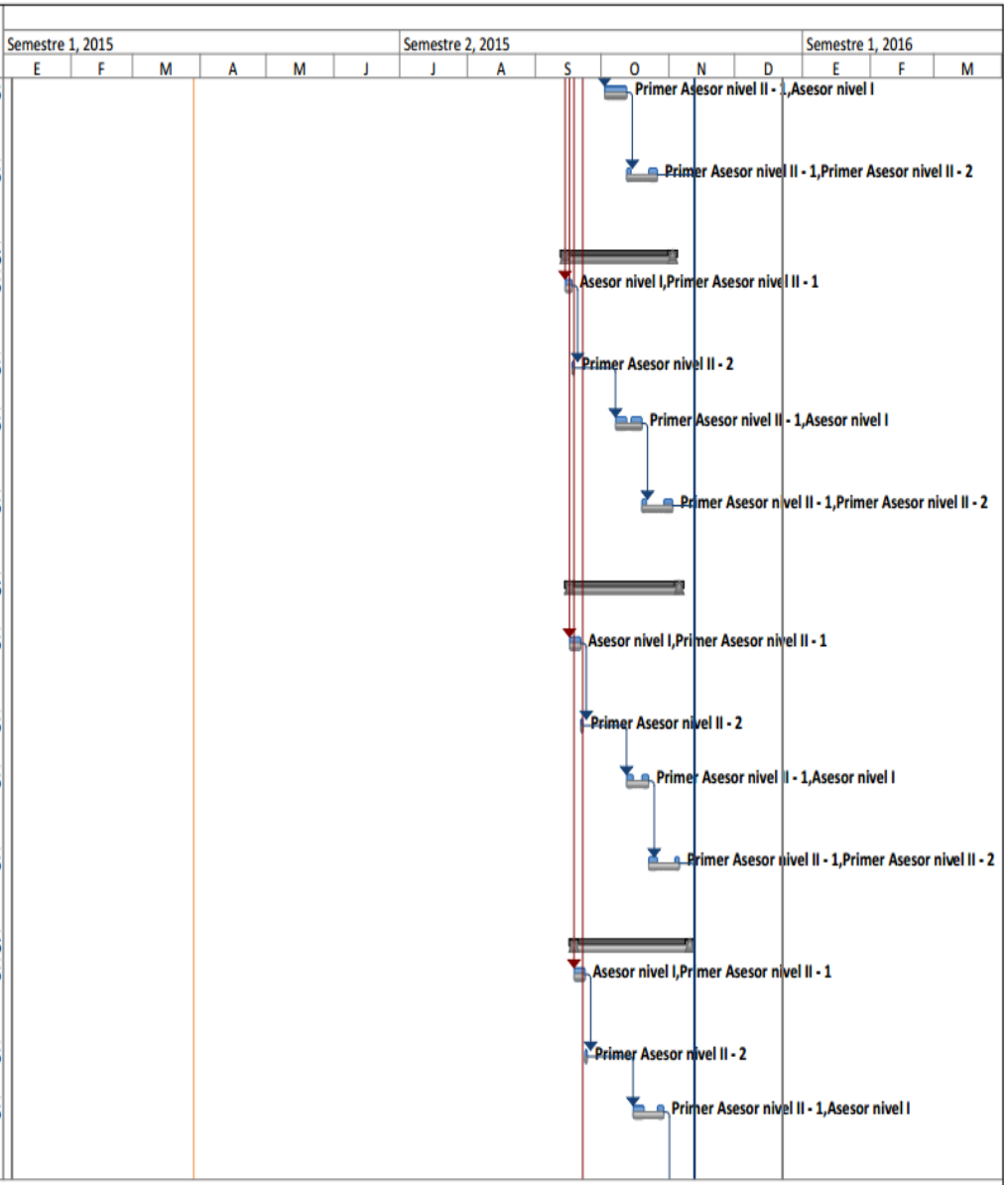
Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
41		1.3.2.2.6	0%	Estimar y validar tamaño y complejidad de los factores de riesgo	lun 27/07/15	mié 05/08/15
42		1.3.2.2.6.1	0%	Cálculo del valor de riesgo asociado a cada activo	lun 27/07/15	mar 28/07/15
43		1.3.2.2.6.2	0%	Identificación de amenazas de los activos	mar 28/07/15	jue 30/07/15
44		1.3.2.2.6.3	0%	Estimación de vulnerabilidad de los	jue 30/07/15	lun 03/08/15
45		1.3.2.2.6.4	0%	Socializar con los responsables los	lun 03/08/15	mar 04/08/15
46		1.3.2.2.6.5	0%	Solicitar respuesta a los responsables sobre los riesgos y vulnerabilidades	mar 04/08/15	mié 05/08/15
47		1.3.2.3	0%	Tratamiento de riesgos	mié 05/08/15	lun 24/08/15
48		1.3.2.3.1	0%	Inventario de activos de la información	mié 05/08/15	lun 10/08/15
49		1.3.2.3.2	0%	Identificacion de los procesos de la cadena de valor de la organizacion	lun 10/08/15	lun 17/08/15
50		1.3.2.3.3	0%	Identificación de Riesgos para cada Activo de	lun 17/08/15	jue 20/08/15
51		1.3.2.3.4	0%	Carta de aceptación de riesgos por parte de la alta	jue 20/08/15	lun 24/08/15
52		**1.4**	**0%**	**Implementación del SGSI**	**lun 24/08/15**	**jue 12/11/15**
53		1.4.1	0%	Politicas de seguridad	lun 24/08/15	mar 25/08/15
54		1.4.2	0%	Organización de la seguridad de la información	mar 25/08/15	jue 03/09/15
55		1.4.2.1	0%	Entrenamiento y entendimiento de los controles	mar 25/08/15	mar 01/09/15
56		1.4.2.2	0%	Aprobar y publicar controles y procedimientos	mar 01/09/15	jue 03/09/15
57		1.4.3	0%	**Aplicación de controles**	jue 03/09/15	jue 12/11/15
58		**1.4.3.1**	**0%**	**Gestion de las comunicaciones y la operación**	**jue 03/09/15**	**vie 06/11/15**
59		1.4.3.1.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	jue 03/09/15	mar 08/09/15
60		1.4.3.1.2	0%	Medir los resultados obtenidos.	mar 08/09/15	vie 11/09/15



Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
61		1.4.3.1.3	0%	Establecer medidas correctivas sobre las debilidades establecidas.	vie 23/10/15	mié 28/10/15
62		1.4.3.1.4	0%	Documentar el control aplicado y la evidencia del control establecida.	mié 28/10/15	vie 06/11/15
63		**1.4.3.2**	**0%**	**Control de acceso**	**jue 03/09/15**	**mié 07/10/15**
64		1.4.3.2.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	jue 03/09/15	lun 07/09/15
65		1.4.3.2.2	0%	Medir los resultados obtenidos.	lun 07/09/15	mar 08/09/15
66		1.4.3.2.3	0%	Establecer medidas correctivas sobre las debilidades establecidas.	jue 24/09/15	mié 30/09/15
67		1.4.3.2.4	0%	Documentar el control aplicado y la evidencia del control establecida.	mié 30/09/15	mié 07/10/15
68		**1.4.3.3**	**0%**	**Sistemas de información, adquisición, desarrollo y mantenimiento**	**lun 07/09/15**	**mié 14/10/15**
69		1.4.3.3.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	lun 07/09/15	jue 10/09/15
70		1.4.3.3.2	0%	Medir los resultados obtenidos.	jue 10/09/15	vie 11/09/15
71		1.4.3.3.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	mar 29/09/15	lun 05/10/15
72		1.4.3.3.4	0%	Documentar el control aplicado y la evidencia del control establecida.	lun 05/10/15	mié 14/10/15
73		**1.4.3.4**	**0%**	**Seguridad de la información en la gestion de incidentes**	**jue 10/09/15**	**lun 26/10/15**
74		1.4.3.4.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	jue 10/09/15	mar 15/09/15
75		1.4.3.4.2	0%	Medir los resultados obtenidos.	mar 15/09/15	mié 16/09/15



Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
76		1.4.3.4.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	vie 02/10/15	lun 12/10/15
77		1.4.3.4.4	0%	Documentar el control aplicado y la evidencia del control establecida.	lun 12/10/15	lun 26/10/15
78		**1.4.3.5**	**0%**	**Cumplimiento**	**lun 14/09/15**	**lun 02/11/15**
79		1.4.3.5.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	lun 14/09/15	jue 17/09/15
80		1.4.3.5.2	0%	Medir los resultados obtenidos.	jue 17/09/15	vie 18/09/15
81		1.4.3.5.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	mié 07/10/15	lun 19/10/15
82		1.4.3.5.4	0%	Documentar el control aplicado y la evidencia del control establecida.	lun 19/10/15	lun 02/11/15
83		**1.4.3.6**	**0%**	**Gestion del plan de continuidad de negocio**	**mié 16/09/15**	**jue 05/11/15**
84		1.4.3.6.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	mié 16/09/15	lun 21/09/15
85		1.4.3.6.2	0%	Medir los resultados obtenidos.	lun 21/09/15	mar 22/09/15
86		1.4.3.6.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	lun 12/10/15	jue 22/10/15
87		1.4.3.6.4	0%	Documentar el control aplicado y la evidencia del control establecida.	jue 22/10/15	jue 05/11/15
88		**1.4.3.7**	**0%**	**Seguridad fisica y ambiental**	**vie 18/09/15**	**mar 10/11/15**
89		1.4.3.7.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	vie 18/09/15	mié 23/09/15
90		1.4.3.7.2	0%	Medir los resultados obtenidos.	mié 23/09/15	jue 24/09/15
91		1.4.3.7.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	jue 15/10/15	jue 29/10/15



Id	Modo de tarea	EDT	% compl	Nombre de tarea	Comienzo	Fin
92		1.4.3.7.4	0%	Documentar el control aplicado y la evidencia del control establecida.	jue 29/10/15	mar 10/11/15
93		1.4.3.8	0%	Seguridad del recurso humano	mar 22/09/15	jue 12/11/15
94		1.4.3.8.1	0%	Establecer normas y métodos para medir el rendimiento de los controles	mar 22/09/15	vie 25/09/15
95		1.4.3.8.2	0%	Medir los resultados obtenidos.	vie 25/09/15	lun 28/09/15
96		1.4.3.8.3	0%	Tomar medidas correctivas sobre las debilidades establecidas.	mar 20/10/15	mar 03/11/15
97		1.4.3.8.4	0%	Documentar el control aplicado y la evidencia del control establecida.	mar 03/11/15	jue 12/11/15
98		1.5	0%	Capacitación	jue 12/11/15	lun 21/12/15
99		1.5.1	0%	Preparación del material de formación y entrenamiento	jue 12/11/15	jue 26/11/15
100		1.5.2	0%	Definición del calendario de formación y entrenamiento	jue 26/11/15	mar 01/12/15
101		1.5.3	0%	Socializar fechas de entrenamient	mar 01/12/15	mié 02/12/15
102		1.5.4	0%	Establecer el sitio de capacitación	mié 02/12/15	vie 04/12/15
103		1.5.5	0%	Agendar al personal que asistira y los temas a tratar en cada	vie 04/12/15	lun 07/12/15
104		1.5.6	0%	Formación y entrenamiento	lun 07/12/15	lun 21/12/15
105		1.6	0%	Reunión de cierre del proyecto	lun 21/12/15	mar 22/12/15
106		1.7	0%	Fin proyecto	mar 22/12/15	mar 22/12/15