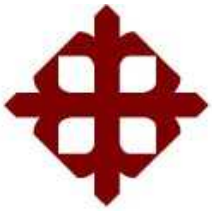


UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

Trabajo de Seminario de Graduación

Previo a la Obtención del Título de:
INGENIERO EN SISTEMAS COMPUTACIONALES

Tema:

Diseñar un modelo de contingencia de sistemas y Telecomunicaciones para las entidades bancarias del Ecuador

Realizado por:

Alberto Guevara / Diana Lopez

Director:

Ing. Xavier Miranda.

Guayaquil, Ecuador
2012

TRABAJO DE SEMINARIO DE GRADUACIÓN

Título

Diseñar un modelo de contingencia de sistemas y Telecomunicaciones para las entidades bancarias del Ecuador

Presentado a la Facultad de Ingeniería, Carrera de Ingeniería en Sistemas Computacionales de la Universidad Católica de Santiago de Guayaquil

Realizado por:

Alberto Guevara / Diana Lopez

Para dar cumplimiento con uno de los requisitos para optar por el Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

Tribunal de Sustentación:

Ing. Xavier Miranda R.
DIRECTOR DEL TRABAJO

Ing. Beatriz Guerrero Y, Mgs.
VOCAL

Ing. César Salazar T, Mgs.
VOCAL

Ing. Lilia Valarezo de Pareja, Mgs.
DECANO DE LA FACULTAD (E)

Ec. Beatriz Guerrero, Mgs.
DIRECTOR DE LA CARRERA(E)

AGRADECIMIENTOS

A Dios por permitirme llegar hasta donde he llegado y hacer realidad mi sueño de realizarme profesionalmente.

A mi familia por el apoyo incondicional al acompañarme a lo largo del camino, brindándome la fuerza necesaria para continuar ya que siempre estuvieron alentándome en los momentos más difíciles de mi carrera, y porque el orgullo que sienten por mi, fue lo que me hizo ir llegar hasta el final.

A mis profesores que me han orientado durante estos años siempre, por su crítica certera, sus palabras de aliento y por impulsarnos a esforzarnos a ser mejores cada día.

Diana López G.

Agradezco primero a Dios por darme la oportunidad vivir para poder contribuir con mi país. A mis padres por el apoyo incondicional a lo largo de la carrera universitaria. Me enseñaron a ser constantes y gracias a ellos puedo cumplir mis objetivos y metas en la vida. Gracias por creer en mí en todo momento.

A los profesores de la carrera por su esfuerzo y dedicación. Siempre me ayudaron a progresar en la vida profesional corrigiendo mis errores y potenciando mis virtudes.

Alberto Guevara V.

DEDICATORIA

Quisiera dedicar este trabajo a mis padres por ser el pilar fundamental de mi vida, porque han sido testigos del esfuerzo invertido, por haberme infundido los valores necesarios a través del tiempo y por creer en mí en todo momento.

A mis amigos por formar parte de mi vida, por compartir conmigo sus alegrías y tristezas y por permitirme crecer a su lado como persona y profesional

A mi compañero de tesis por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de este proyecto

A mis maestros gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

A Daniel Parra por su paciencia su estímulo, su apoyo constante. Gracias por hacerme poner los pies sobre la tierra y sobre todo por el cariño y amor que me brindas a cada instante

Diana López.

Dedico este documento a las personas que me apoyaron en todo momento. A mis padres por darme las facilidades de estudiar para ser un profesional y poder cumplir mis metas. Jamás podría llegar tan lejos sin su ayuda. Cumplieron con su labor que les costó mucho esfuerzo pero sabían que poco a poco estaban construyendo un profesional y un hombre con valores y principios éticos. Gracias por darme la mejor vida que un hijo puede tener. Jamás me falto nada y es hora que yo pueda retribuir por todo su esfuerzo y dedicación.

También dedico a mi novia que me recuerda quien soy cuando estoy perdido, me que enseña a soñar y luego a luchar por ese sueño. Es mi espada en la batalla y a su lado no hay guerra que no pueda ganar.

A mis amigos de mi infancia que mal llamado es decir amigos pues son realmente mis hermanos. Dios no me dio un hermano de sangre pero me dio muchos hermanos de vida. Los tengo en mi mente en cada momento y no me imagino cómo sería mi vida sin haberlos conocido.

Por último quiero agradecer a mis compañeros del trabajo. Es un privilegio estar rodeado todos los días de los mejores ingenieros del Ecuador. Me enseñaron mucho en la parte técnica y humana y nunca me alcanzará el tiempo para agradecerles todo lo que han contribuido en mi vida profesional.

Alberto Guevara V.

PREFACIO

El presente trabajo del Seminario de Graduación de la Carrera de Ingeniería en Sistemas Computacionales de la Facultad de Ingeniería, nace del Convenio Marco de Colaboración entre la Universidad de Valencia- España y la Universidad Católica de Santiago de Guayaquil- Ecuador cuya finalidad es la de formar a sus alumnos en el manejo de Proyectos en su fase inicial y posteriormente los alumnos que estén interesados en profundizar con este conocimiento y mejores prácticas lo podrán realizar a través de la Maestría en Dirección y Administración de Proyectos.

El presente trabajo consiste en la presentación de un proyecto dividido en dos partes:

Parte I: Propuesta del Tema el cual consiste en seguir la metodología de Investigación aplicada al proyecto planteado por los estudiantes siguiendo la estructura propuesta por la Universidad Católica de Santiago de Guayaquil.

Parte II: Desarrollo del proyecto final de la Universidad de Valencia, de acuerdo a la elección del proyecto aprobado por la Universidad de Valencia y siguiendo un proceso desde la perspectiva de Dirección de Proyectos.

ÍNDICE GENERAL

Índice de Contenido

Parte II.- Desarrollo del proyecto.

Índice de Cuadros

Índice de Gráficos

INTRODUCCIÓN

El presente tema ha sido elaborado de acuerdo a las necesidades más relevantes en las entidades bancarias actuales, el mismo ayudara al personal del área de TI a responder ante contingentes o desastres que se presenten y atenten contra la correcta operatividad del banco. Nuestro proyecto abarca las buenas prácticas de la dirección de proyecto indicadas en el PMBOK. Se desarrollan las fases de inicio, planificación. Las fases de seguimiento y control no están desarrolladas en el presente documento. Para asegurar la calidad de nuestro proyecto se utilizaran estándares internacionales con respecto a la seguridad de la información y continuidad del negocio.

PARTE I

Propuesta del Tema

CAPÍTULO 1

Problema de Investigación

1.1 Enunciado del Problema

En las entidades bancarias los mayores problemas se originan por varios factores tales como:

- Un diseño ineficiente en el plan de contingencia.
- El robo de información por hackers o piratas informáticos es una de las principales amenazas que atraviesa el sistema bancario.
- La falta de mantenimiento periódico en la infraestructura, ocasionando el deterioro de los mismos.
- Falta de análisis en la selección del proveedor de telecomunicaciones.
- La carencia o un mal diseño de esquema de respaldo de información.

El problema de la falta de un buen diseño de contingencia ocasiona problemas directos en todas las áreas.

Las razones por las cuales no se cuenta con un buen plan de contingencia podrían ser:

- Falta de capacitación del personal del área de tecnología.
- Falta de presupuesto al plan de contingencia.

- Desconocimiento del concepto de un plan de contingencia BCP (Business Continuing Planning)
- Mala asignación de recursos para el plan de contingencia.

1.2 Formulación del Problema

El problema del robo de la información podría ocasionar una pérdida de imagen de la entidad financiera lo que genera la desconfianza de los clientes actuales y potenciales

La falta de un mantenimiento preventivo podría ocasionar la perdida de operatividad de los sistemas y de la red.

El problema de tener un deficiente diseño de esquema de respaldo de información puede generar falsas expectativas en el plan de contingencia.

Un problema al elegir un mal proveedor es tener constantes incidentes con los servicios que nos brinda.

1.3 Justificación y Delimitación.

1.3.1 Justificación.

Todos los sistemas están propensos a fallos ya sea por algún ataque externo o daño de hardware o software. Algunos de estos fallos toman días y hasta semanas generando inconformidad en los clientes. No existe un análisis de las incidencias que pueden ocurrir y peor aun estar prevenidos.

Adicional la gerencia de las instituciones bancarias necesitan tener los sistemas informáticos como los sitios web para realizar las transacciones en línea, de esta manera tratar de equilibrar el tránsito de los clientes con el objetivo de minimizar el costo de operación de las sucursales. Si un usuario puede realizar transacciones desde su hogar, oficina o en cualquier lugar del mundo ¿por qué la banca por internet no ha logrado un éxito en el Ecuador?

Los constantes ataques a diversas entidades públicas y privadas son cada día más frecuentes en nuestro país.

En nuestro caso las entidades bancarias son objetivos principales de los hackers que prueban las vulnerabilidades de los sistemas informáticos.

Una de las razones es que el recurso del internet es inseguro y tanto el usuario como el banquero tienen temor en utilizar estas herramientas informáticas pero con un estudio de vulnerabilidad y contingencias se podrá recuperar durante una falla en los sistemas.

. Otro recurso muy importante es la disponibilidad de la salida al internet otorgado por el proveedor de telecomunicaciones. Los servidores Web deben estar operativos las 24 horas los 365 días del año y si un proveedor sufre alguna caída la entidad bancaria debe tener un plan de contingencia para re direccionar el trafico a otro proveedor. Es necesario hacer un correcto análisis de los proveedores de internet y datos en el Ecuador y así minimizar el impacto por la falla de este agente externo.

1.3.2 Delimitación.

El proyecto abarca el diseño de un modelo de contingencia en sistemas informáticos y telecomunicación más no la implementación del mismo. Este diseño ayudará a la elaboración de un posterior BCP de la institución financiera. La metodología del BCP abarca la seguridad física y lógica de los activos de información pero solo se va a contemplar la seguridad lógica.

Mediante la investigación se determinará el mejor modelo basándose en hechos científicos e implementaciones realizadas en otros proyectos. Se analizará las soluciones que existen en el mercado y cuáles son las fortalezas y debilidades.

Se estudiará las vulnerabilidades más frecuentes de los sistemas informáticos bancarios y los mecanismos de recuperación cuando un incidente de seguridad se presenta.

Se presentará múltiples alternativas de proveedores de servicios de telecomunicaciones que existen en Guayaquil. Cada proveedor posee una solución para realizar un respaldo manual o automático el cual será analizado mas no implementado en este proyecto.

1.4 Objetivos

1.4.1 Objetivo General.

Diseñar un plan adecuado y real con los activos necesarios para asegurar el funcionamiento del modelo de negocios y la operatividad en las Entidades

Bancarias ante cualquier incidente relacionado a sistemas y telecomunicaciones.

1.4.2 Objetivos Específicos.

- Identificar los principales problemas que afectan a las áreas de sistemas y telecomunicaciones
- Diseñar y estructurar el mejor plan de contingencia para las Entidades Bancarias
- Dar a conocer al personal encargado del Plan de Contingencia las principales vulnerabilidades que afectan al área de sistemas y redes de estas entidades.
- Identificar los recursos mínimos con los que debe contar la institución bancaria.
- Evaluar los impactos financieros y operacionales que un desastre puede causar en las operaciones de la organización, sus áreas y su infraestructura.
- Explicar eventos y factores de Riesgo para realizar un plan de respuesta a riesgo.

CAPITULO 2

Marco referencial

2.1 Antecedentes

Como antecedentes tenemos las fallas del sistema del Banco de Guayaquil que se presentaron el viernes 15 de julio del 2011. Según los datos del diario El Universo el inconveniente se presentó en el software de la Empresa IBM. El sistema informático del banco estuvo inestable por varios días.

Esto evidencia que en la actualidad son pocas las instituciones del Sistema Financiero que tienen infraestructuras y procesos alternos, para funcionar ante situaciones de desastre y que puedan continuar con la operación durante el período de tiempo necesario para restaurar los procesos, sistemas o personal afectado por estos acontecimientos.

2.2 Marco teórico

Como se indico las entidades bancarias del Ecuador están propensas a los ataques de piratas informáticos y es necesario tener un plan de acción antes, durante y después del incidente de seguridad. Para estar prevenidos a cualquier ataque seguiremos la metodología del BCP del ISO 27001 enfocado la contingencia de sistemas informáticos y telecomunicaciones.

La implementación de normas como la ISO 27001 que se integra perfectamente a sistemas de gestión sobre calidad ofrece mayor seguridad de la información y los siguientes beneficios:

- Reduce el riesgo de pérdida, robo o corrupción de información.
- Permite establecer una metodología de gestión de la seguridad clara
- Mejora la imagen de la empresa, diferenciándose con respecto a la competencia.
- Permite a la empresa ganar cuota de mercado gracias a la confianza que genera entre los clientes y socios estratégicos.
- Permite continuar con las operaciones necesarias del negocio tras incidentes de gravedad.
- Permite a la empresa medir la eficacia de su sistema de gestión de acuerdo con normas nacionales e internacionales a través de la certificación de terceros.
- Establece los cimientos a través de los que mejora continuamente sus procesos internos y refuerza la habilidad de la organización para

alcanzar los objetivos estratégicos, en este caso la seguridad de la información.

También es importante tener como base un concepto de BCP amoldado a la estructura de la compañía. El plan de continuidad de negocio es esencial para proseguir con las actividades criticas la misma, en el caso en el que se presentara un evento inesperado que pudiese comprometer los procesos de operación o pongan en riesgo el flujo de trabajo de la entidad bancaria. Dependiendo el presupuesto asignado se investigará la mejor solución para un incidente de seguridad. Por medio de simulacros se probará la eficacia de los modelos planteados para tener tiempos estimados en la recuperación de los sistemas informáticos.

Esta metodología es muy general pero en este proyecto será orientado a establecer un adecuado modelo de contingencia para la prevención un incidente como el daño de hardware o software.

En este proyecto resaltaremos la necesidad de contar con estrategia que permitan realizar un análisis de riesgos para poder detectar las vulnerabilidades existentes y realizar la mitigación del mismo.

2.2.1 Riesgos potenciales de los sistemas bancarios.

Actualmente existes varios riesgos que afrontan los sistemas informáticos y el primer paso es identificar los activos de información relevantes de la entidad financiera. Cada activo de información debe ser protegido, buscar

posibles fallos de seguridad y determinar cuál sería el impacto en el banco si se genera un incidente.

Posterior es necesario determinar los pasos necesarios para minimizar o anular la ocurrencia de estos incidentes que pueden generar el daño. En caso de incidente mayor debemos generar un plan de contingencia para reponernos al daño o minimizar las perdidas ocasionadas.

De igual manera los CPE o el enrutador del proveedor de telecomunicaciones son activos de información que puede sufrir un ataque preveniente de un hacker.

En resumen se puede identificar los siguientes activos de información:

Hardware: Servidores de correo, Servidores web.

Software y utilitarios: Aplicaciones, antivirus

Equipos de telecomunicaciones: switches, router, firewall, Access Point, Teléfonos IPs

Estos activos son susceptibles a los ataques informáticos por este motivo es necesario incrementar las seguridades ya que se maneja información confidencial de los clientes. También los datos financieros como saldos y transacciones debes estar resguardados para evitar modificaciones y fraudes en las cuentas de ahorro y corriente de los clientes finales. Estos riesgos de alteración de información son riesgos potenciales que afrontan todos los días los bancos a nivel nacional e internacional.

2.2.2 Fuentes de vulnerabilidades.

Existen muchas vulnerabilidades que pueden ser explotadas por agentes internos como externos.

Instalación de software espía o de comportamiento errático con el fin de dañar la operación de los sistemas informáticos. Los servidores críticos como correo electrónico, servidores web y los servidores de aplicaciones deben tener software esenciales para el servicio que proveen. No deben tener otros programas que afecten el rendimiento o deben huecos de seguridad. Cualquier hacker puede realizar un escaneo de puertos y detectar vulnerabilidades.

De igual manera para los equipos de telecomunicaciones deben tener puertos bloqueados mediante ACL para restringir el acceso y que solo el personal calificado pueda ingresar y realizar cambios o configuraciones.

Otra fuente de falla que es muy complicado de anticipar es el daño de hardware. Todos los equipos deben tener un mantenimiento preventivo para evitar inconvenientes en un futuro. Los discos duros y el procesador central de los servidores de aplicaciones o base de datos deben ser monitoreados periódicamente.

También el hardware de la red puede sufrir daños a corto o largo plazo. Se puede presentar la falla del cableado de red, equipos conmutadores y los routers.

La información que viaja sobre una red de datos esta propensa a la intercepción de información confidencial de una entidad bancaria. Si enviamos datos a través de un medio inseguro como es el internet tenemos altas probabilidades que los piratas informáticos intercepten datos confidenciales del banco. Los programas sniffer como el wire shark puede leer contraseñas, documentos transmitidos, correos electrónicos enviados, etc.

Con esta información fácilmente la red de una sucursal bancaria puede estar comprometida haciendo que una contingencia resulte más difícil en ejecutarla.

2.3 Marco Conceptual

BCM (Business Continuity Managment): Se trata de una metodología interdisciplinaria con la finalidad de mantener la continuidad del negocio durante un desastre, la misma que contempla todas las medidas preventivas y de recuperación para cuando se produzca algún incidente que afecte al negocio

Superintendencia de Bancos y Seguros del Ecuador: Institución reguladora de las entidades financieras del Ecuador.

Hackers: Expertos en salvaguardar o violar la seguridad de la empresa, esto puede afectar de manera positiva o negativa a los sistemas Informáticos de la corporación

BIA (Business Impact Analysis): Análisis de Impacto del Negocio, es la actividad de gestión de continuidad del Negocio que identifica los servicios críticos del negocio. Adicionalmente define los procesos de recuperación para los servicios de TI

SANS Institute: Institución que reúne información sobre todo lo referente a seguridad lógica, las mismas que son actualizadas en referencia a las ultimas vulnerabilidades más frecuentes encontradas alrededor del mundo

2.4 Marco Legal

La Superintendencia de Bancos y Seguros mediante la Resolución No. JB-2005-834 y posteriormente con la Resolución JB-2008-1202 se dispuso que las instituciones financieras implementen planes de continuidad de negocios a fin de garantizar su trabajo en forma permanente y así minimizar las pérdidas en casos de interrupción de sus operaciones, mediante la aplicación de planes de contingencia que permitan ejecutar los respectivos planes de acción.

El estándar BS 25999, para la gestión de continuidad de negocio (Business Continuity Management-BCM), que ayuda a minimizar el riesgo de interrupciones por diferentes tipos de desastres o impactos.

CAPITULO 3

Metodología

3.1 Tipo de investigación

La investigación de nuestro proyecto es pre experimental porque se tiene un mínimo control en las variables o componentes que utilizaremos para la elaboración del proyecto. Con este método se tendrá un primer acercamiento al problema a de investigación real ya que pocos estudios han profundizado este tema.

Este método permite estudiar las relaciones causa efecto que se obtiene al Aplicar los Estandares de continuidad del negocio en una entidad financiera.

Al reducir el riesgo de incidente informático tiene un efecto positivo en los Activos de información del banco.

Una de las causas de los incidentes de seguridad es la falta de actualización de nuevos métodos de ataque a los sistemas informáticos. Estas aplicaciones manejan información financiera que cualquier hacker desea alterar. Esto genera un efecto negativo en los informes contables que desarrolla la entidad financiera y adicional una mala imagen hacia los acreedores del banco.

En el contenido de este proyecto vamos a desarrollar aproximaciones para diseñar un modelo óptico para las instituciones financieras del Ecuador. El

fin de este proyecto es explorar el campo informático de las entidades financieras por el motivo que no existe información sobre las infraestructuras que poseen los bancos del Ecuador.

3.2 Diseño de la investigación

El proyecto consiste en una propuesta, plan y modelo para la solución de los incidentes de seguridad lógica de las entidades financieras del Ecuador.

Por esta razón nuestro diseño de investigación será proyectiva por las planificaciones que realizaremos a lo largo del documento. Esta metodología tiene algunas similitudes con el PMBOK con respecto a las áreas de conocimiento. La investigación proyectiva tiene como fin alcanzar los objetivos y las metras trazadas durante el proceso del proyecto. Estos objetivos se establecen en el PMBOK en la parte de iniciación.

Otras características de la investigación proyectiva son que debe tener un proceso sistemático de búsqueda e indagación que requiere la descripción del problema, el análisis, la comparación, la explicación y la predicción. Con el PMBOK establecemos la problemática y realizamos un análisis para poder satisfacer las necesidades. En varias etapas del proyecto se compara con otros proyectos para tener una referencia de costos o de tiempo. Así tendremos una predicción estimada de la finalización del proyecto.

Diseño y elaboración de planes que beneficiarán para el buen funcionamiento de la red de datos y sistemas. Para cumplir con los objetivos trazados tendremos como normas la ISO 27001 y BCP para garantizar un modelo ideal de seguridad y disponibilidad.

Nuestra propuesta contiene la descripción del problema, análisis de las posibles fallas de seguridad, la comparación con las normas más relevantes de la seguridad informática y por último la explicación de todas las actividades que es necesario realizar para completar un modelo óptico para el sistema financiero del Ecuador. Al conocer esta información que nos proporciona la investigación proyectiva nos acercaremos a la realidad de las operaciones bancarias para detectar las posibles vulnerabilidades.

3.3 Población y muestra

Los datos se tomaron con muestreo no probabilístico por conveniencia para el desarrollo de nuestra investigación

La población es el sistema bancario del Ecuador de los cuales se tomará como muestra las 4 instituciones más representativas del Ecuador las mismas que se encuentran localizadas en la ciudad de Guayaquil para realizar un análisis más profundo sobre las vulnerabilidades de sistemas y telecomunicaciones.

Los criterios de selección son:

- Variación del Capital Pagado.
- Variación de Ingresos.
- Variación de Egresos.
- Variación de las Utilidades.

Cuadro 1. Variación Capital Pagado.

BANCOS PRIVADOS
VARIACION CAPITAL PAGADO
(miles)

	dic-10	dic-11	VARIACION ABSOLUTA	VARIACION RELATIVA
BP PICHINCHA	358.000	421.500	63.500	17,7%
BP GUAYAQUIL	156.000	181.000	25.000	16,0%
BP PACIFICO	200.734	223.144	22.410	11,2%
BP BOLIVARIANO	102.540	115.790	13.250	12,9%
BP PRODUBANCO	135.000	148.000	13.000	9,6%
BP INTERNACIONAL	99.000	110.000	11.000	11,1%
BP AUSTRO	50.000	54.000	4.000	8,0%
BP PROMERICA	33.695	36.624	2.929	8,7%
BP TERRITORIAL	10.969	12.969	2.000	18,2%
BP MACHALA	30.000	32.200	2.200	7,3%
BP GENERAL RUMIÑAHUI	20.630	22.505	1.875	9,1%

Fuente: Superintendencia de Compañías y Seguros
Elaborado por: Roberto Muñoz Bermeo.

El análisis compara la variación del capital pagado del mes de diciembre del año 2010 y el año 2011. Podemos observar que el banco del Pichincha y el banco de Guayaquil lideran la variación del capital pagado

Cuadro 2. Variación de Ingresos.

BANCOS PRIVADOS
VARIACION DE INGRESOS
(miles)

	dic-10	dic-11	VARIACION ABSOLUTA	VARIACION RELATIVA
BP PICHINCHA	683.700	880.789	197.089	28,8%
BP GUAYAQUIL	296.785	396.995	100.210	33,8%
BP PRODUBANCO	158.756	189.988	31.233	19,7%
BP PACIFICO	224.338	253.770	29.432	13,1%
BP BOLIVARIANO	132.221	155.995	23.774	18,0%
BP INTERNACIONAL	132.579	154.353	21.774	16,4%
BP AUSTRO	99.585	118.863	19.278	19,4%
BP UNIBANCO	72.346	83.118	10.772	14,9%
BP PROMERICA	46.335	56.707	10.372	22,4%
BP DELBANK	3.152	12.559	9.406	298,4%
BP LOJA	23.339	32.516	9.177	39,3%

Fuente: Superintendencia de Compañías y Seguros
Elaborado por: Roberto Muñoz Bermeo.

Nuevamente el banco Pichincha lidera la variación de ingresos junto al banco de Guayaquil.

Cuadro 3. Variación de Egresos.

BANCOS PRIVADOS
VARIACION DE EGRESOS
(miles)

	dic-10	dic-11	VARIACION ABSOLUTA	VARIACION RELATIVA
BP PICHINCHA	604.605	784.268	179.663	29,7%
BP GUAYAQUIL	252.383	298.893	46.509	18,4%
BP PACIFICO	188.326	209.173	20.847	11,1%
BP PRODUBANCO	136.257	156.168	19.910	14,6%
BP BOLIVARIANO	111.194	130.480	19.285	17,3%
BP AUSTRO	86.505	103.089	16.584	19,2%
BP INTERNACIONAL	112.198	127.775	15.577	13,9%
BP COOPNACIONAL		10.807	10.807	0,0%
BP UNIBANCO	66.587	75.704	9.118	13,7%
BP PROMERICA	42.719	50.697	7.978	18,7%
BP D-MIRO S.A.		7.322	7.322	0,0%

Fuente: Superintendencia de Compañías y Seguros
Elaborado por: Roberto Muñoz Bermeo.

Por la gran cantidad de clientes el banco Pichincha y Guayaquil son los que más gastos registran.

Cuadro 4. Variación de las utilidades

BANCOS PRIVADOS
VARIACION DE LAS UTILIDADES
(miles)

	dic-10	dic-11	VARIACION ABSOLUTA	VARIACION RELATIVA
BP GUAYAQUIL	44.402	98.102	53.701	120,9%
BP PICHINCHA	79.095	96.521	17.426	22,0%
BP PRODUBANCO	22.498	33.821	11.322	50,3%
BP PACIFICO	36.011	44.597	8.585	23,8%
BP LLOYDS BANK	-8.510		8.510	-100,0%
BP INTERNACIONAL	20.381	26.578	6.197	30,4%
BP BOLIVARIANO	21.027	25.516	4.489	21,3%
BP SOLIDARIO	2.768	7.028	4.260	153,9%
BP CITIBANK	2.359	5.704	3.345	141,8%
BP LOJA	3.208	6.007	2.799	87,3%
BP AUSTRO	13.080	15.774	2.694	20,6%
BP PROMERICA	3.616	6.010	2.394	66,2%

Fuente: Superintendencia de Compañías y Seguros
Elaborado por: Roberto Muñoz Bermeo.

Este factor es determinante. El banco de Guayaquil registra el más alto índice de utilidades en el sistema financiero del Ecuador.

3.4 Técnicas e instrumentos para obtención de información

La técnica a utilizar será la entrevista estructurada la cual se aplicará a los jefes de las áreas de sistemas y telecomunicaciones de las 4 instituciones bancarias seleccionadas.

3.5 Procesamiento y análisis de la información

Los resultados de la entrevista se tabularán en una hoja electrónica de cálculo para poder identificar los problemas comunes de las instituciones bancarias seleccionadas para este proyecto.

Con las entrevistas se busca establecer si existen planes de contingencia, estándares de calidad o certificaciones que garanticen el correcto funcionamiento de los procesos internos de la entidad bancaria. Adicionalmente la postura de la institución para otorgar información necesaria para acciones de mejoras.

Las entidades bancarias conocen la metodología del BCP pero no realizan estudios periódicos, ni existen consultorías de agentes externos para comprobar la efectividad del mismo. Dicho hecho es necesario, para la mejora continua de la seguridad de los sistemas Bancarios

CAPÍTULO 4

Plan de trabajo.

Se realizarán las siguientes actividades identificadas a continuación en un periodo aproximado de 1 mes y 5 días.

Cuadro 5. Plan de trabajo de la investigación.

Actividades	Duración (dias)
Investigación del entorno bancario	7
encuestas de aceptación sistema bancario de Guayaquil	5
tabulación de resultados	2
Selección de los bancos más representativos en el entorno a testear	2
Visualización del entorno	
visita a entidad bancaria	3
coordinación de entrevista	1
Selección de técnica de investigación	
Formulación y Estructuración de la Entrevista	2
contacto vía telefónica con los jefes de sistemas y de infraestructura	3
Entrevista de Jefes	7
Tabulación de resultados	3

Elaborado por: Autores

PARTE II

Diseñar un modelo de contingencia de sistemas y telecomunicaciones para las Entidades Bancarias del Ecuador

CAPÍTULO 5

Administración del Proyecto.

5.1 Iniciación.

5.1.1 Seleccionar al director del Proyecto.

Para la selección del director del proyecto nos enfocamos en que tenga habilidades para la comunicación con el equipo de trabajo y liderazgo para llevar el proyecto adelante.

5.1.2 Determinar la cultura de la compañía y los sistemas existentes.

Determinar la cultura de la empresa fue complicado por las restricciones para obtener la información. Pudimos constatar los sistemas informáticos basados en software de IBM para las transacciones bancarias que genera grandes inconvenientes por su complicada administración y escaso soporte a nivel local. Con respecto a las telecomunicaciones su proveedor es Telconet S.A por la cobertura que tiene a nivel nacional.

5.1.3 Dividir el proyecto en grandes fases.

Por la complejidad y lo extenso del proyecto que nos fue encargado lo dividimos en varias fases para poder cumplir con el objetivos trazados por la dirección de informática del banco.

Primero realizaremos un levantamiento de información para detectar las vulnerabilidades en los sistemas de informáticos. Adicional la información que viaja en la red de datos es crítica y debe ser encriptación para evitar que personal no autorizado acceda a los datos de los clientes. Luego de detectar las vulnerabilidades y proyectar el flujo de transacciones de la entidad bancaria es necesario sustentar el nuevo equipamiento que es necesario adquirir para el correcto funcionamiento. A continuación es imprescindible tener la seguridad perimetral para evitar la fuga de información. Ahora que tenemos claro el funcionamiento y los procesos generados por los sistemas informáticos, elaboramos la contingencia en caso de falla de software o hardware. Para los servicios de telecomunicaciones es mandatorio tener como mínimo 2 proveedores para asegurar la disponibilidad de dicho servicio. Seguiremos con la elaboración del BCP para los sistemas informáticos y de telecomunicaciones. Para finalizar tendremos un plan de mantenimiento preventivo para los sistemas informáticos y los equipos de telecomunicaciones.

5.1.4 Lista de Stackeholders

Usuarios Finales: Los Clientes son interesados ya que se esta asegurando la calidad del servicio que recibirán

Directiva: La Directiva podría aprobar o no el proyecto que ha sido generado a consecuencia del levantamiento de información, o restringir el acceso a información necesaria para la creación del BCP.

Proveedor del servicio de internet: ya que las regulaciones hechas pueden afectar la relación entre el proveedor y la institución financiera.

Entidades Reguladoras: Creación de leyes que puedan truncar el progreso del proyecto.

5.1.5 Desarrollar Estrategias para los Stackeholders

Debe existir una muy buena comunicación con nosotros en reuniones periódicas en las que nos permitan indicar los cambios que podrían llegar a darse, y las opciones que tenemos para mejorar el servicio, con los recursos que ellos puedan proveernos.

5.1.6 Acta de Constitución del Proyecto.

Para quedar formalmente establecido el proyecto es necesario generar el acta de constitución del proyecto. Este documento es generado por el patrocinador del proyecto.

Ver Anexo [1]

5.2 Planificación del proyecto.

5.2.1 Enunciado del Alcance

Justificación del alcance del proyecto:

La dirección de informática de las entidades bancarias desea garantizar la contingencia de los sistemas de información y de telecomunicaciones para garantizar la seguridad lógica de los activos de información. Diseñar un modelo para garantizar el equipamiento mínimo que debe adquirir para entrar a operaciones.

Delimitación del alcance del proyecto:

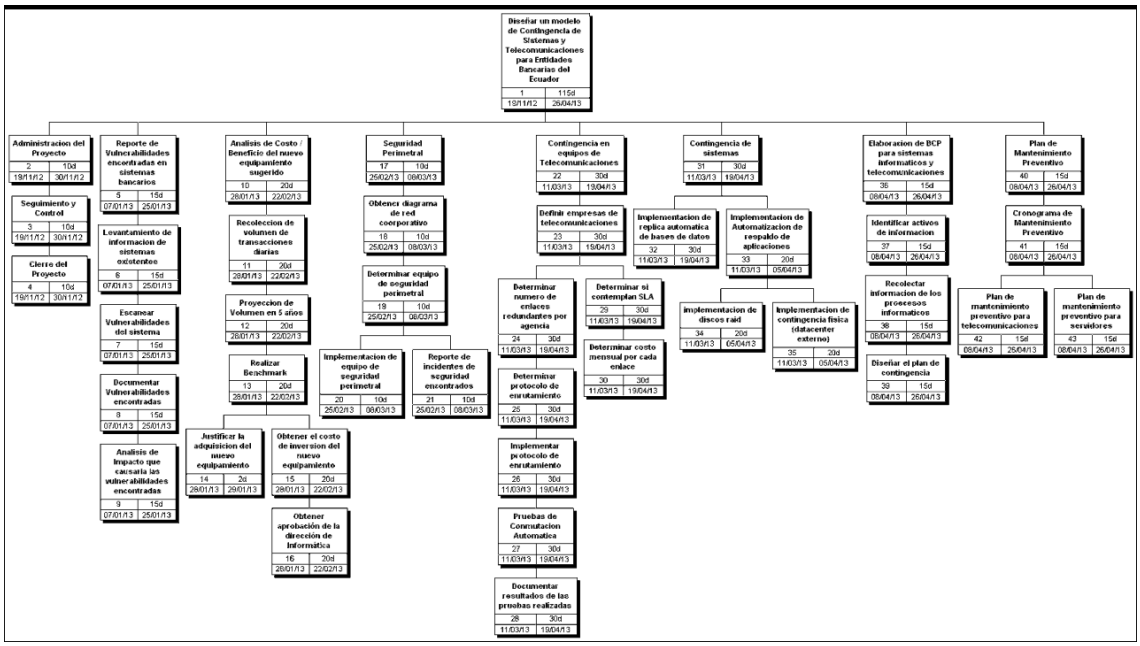
El cliente obtendrá un estudio de análisis de vulnerabilidades existentes en los sistemas informáticos implementados en la actualidad para luego realizar actualizaciones o correctivos. Implementar seguridad perimetral en las agencias y sucursales con el fin de contrarrestar ataques informáticos entro de la red y fuera de la red corporativa. El producto contempla mitigar ataques informáticos como el ping de la muerte, envío y recepción de spam y phishing de la página web. A nivel de telecomunicaciones el implementar respaldo automático en el servicio de transmisión de datos entre las agencias y Matriz. En cada Agencia deberán constar por lo menos 2 proveedores de telecomunicaciones para llevar a cabo la contingencia. El cableado estructurado será testeado y certificado bajo las normas pertinentes. Realizaremos un estudio de las transacciones diarias, mensuales y anuales para la correcta adquisición del Hardware para levantar los sistemas

informáticos que usaran los clientes de la Banca en línea para así garantizar el funcionamiento de 24*7.

Se elaborara un plan de mantenimiento preventivo del hardware adquirido para maximizar la inversión realizada.

5.2.1.1Crear la EDT y el diccionario de la EDT.

Grafico 1. EDT del Proyecto.



Elaborado por: Autores.

Ver Anexo [2]

5.2.1.2 Diccionario de La EDT

1.2	**Reporte de Vulnerabilidades encontradas en sistemas bancarios**
Descripción	Documentación con la evidencia de vulnerabilidades potenciales que existen en los sistemas informáticos de la entidad bancaria.
Actividades	• Presentación a la dirección de informática las vulnerabilidades de los sistemas informáticos. • Procesar la información generada de las tareas predecesoras y realizar cuadros estadísticos del incremento de los incidentes de seguridad presentados.
Duración	12 días
Responsable	Ing. en Sistemas

1.2.1	**Levantamiento de Información de sistemas existentes.**
Descripción	Se recopila los datos e información de los sistemas en producción de la entidad bancaria.
Actividades	• Se solicita la documentación de cada sistema en producción del banco • Si no existe se genera los documentos en conjunto con la dirección de informática. • Elaborar el diagrama de flujo de trabajo de los sistemas informáticos. • Documentar el sistema operativo los servidores en producción. • Documentar la herramienta de base de datos que está en producción.
Duración	1 día.
Responsable	Ing. en Sistemas

1.2.1.1	**Escanear vulnerabilidades del sistema**
Descripción	Con herramientas informáticas se detectará las posibles vulnerabilidades en los sistemas informáticos y telecomunicaciones.
Actividades	• Realizar Nmap para detectar los puertos TCP y UDP que estén abiertos. • Utilizar herramientas de network protocol analyzer para revisar la información que viaja en red de datos. • Generar reporte final con las vulnerabilidades existentes.
Duración	1 día.
Responsable	Ing. en Sistemas

1.2.1.1.1	**Documentar Vulnerabilidades encontradas**
Descripción	Se genera toda la documentación sobre el reporte de vulnerabilidades y los posibles parches de seguridad. Se establece todos los riesgos que tienen los sistemas informáticos.
Actividades	• Verificar las vulnerabilidades en SANS Institute. • Documentar parche de seguridad sugerido. • Establecer software de encriptación de datos para estaciones de trabajo en la red corporativa.
Duración	1 día.
Responsable	Documentador Líder

1.2.1.1.1.1	**Análisis de Impacto que causaría las vulnerabilidades encontradas.**
Descripción	Se realizará un análisis del impacto que causaría un incidente de seguridad lógica con las vulnerabilidades encontradas en los sistemas en producción.
Actividades	• Identificar y cuantificar la perdía de información que causaría cada vulnerabilidad encontrada. • Cuantificar la fuga de información por accesos no deseados. • Cuantificar la pérdida de imagen de la entidad bancaria por un hackeo informático. • Establecer el tiempo que tomaría retomar los servicios afectados.
Duración	9 días.
Responsable	Ing. Sistemas

1.3	**Análisis de Costo / Beneficio del nuevo equipamiento sugerido.**
Descripción	Se sustenta todo el equipamiento mínimo sugerido para poder operar en la entidad bancaria.
Actividades	• Verificar que el equipamiento sugerido sea acorde con las necesidades de seguridad de la entidad bancaria. • Obtener el costo total del equipamiento y como determinar el beneficio para la organización durante 3 años.
Duración	30 días.
Responsable	Administrador del proyecto.

1.3.1	**Recolección de volumen de transacciones diarias.**
Descripción	Se realizará un estudio del todo el flujo de trabajo que tienen los servidores y aplicaciones en producción.
Actividades	• Monitoreo de CPU y memoria Ram de los servidores en producción. • Verificar el consumo de ancho de banda en la red corporativa y agencias bancarias. • Determinar saturación de servidores y equipos de telecomunicaciones durante horas pico o al hacer procesos internos al final del día.
Duración	15 días.
Responsable	Documentador

1.3.1.1	**Proyección en volumen de transacciones a 5 años**
Descripción	Se realizará un análisis estadístico para determinar el flujo de trabajo en 5 años.
Actividades	• Identificar el crecimiento de clientes que utilizan plataformas bancarias. • Discutir sobre la proyección del volumen de transacciones a 5 años • Determinar los factores que influyen en el incremento de las transacciones en línea.
Duración	1 día.
Responsable	Administrador del proyecto.

1.3.1.1.1	**Realizar Benchmark**
Descripción	Se define al Benchmark como la técnica para medir el rendimiento en los sistemas y componentes físicos.
Actividades	• Establecer el rendimiento de los sistemas existentes. • Especificar el benchmark de los nuevos sistemas y comparar con las aplicaciones en producción. • Documentar las pruebas realizadas y establecer el porcentaje de rendimiento.
Duración	1 días.
Responsable	Administrador del proyecto

1.3.1.1.1.1	**Justificar la adquisición del nuevo equipamiento.**
Descripción	Se justifica todo el nuevo equipamiento sugerido para la entidad financiera.
Actividades	• Documentar las marcas, modelos y especificaciones técnicas del nuevo equipamiento. • Verificar que cumplen con los requerimientos establecidos en las especificaciones técnicas del fabricante. • Especificar por cada equipo que servicio se va a implementar.
Duración	3 días.
Responsable	Ing. en infraestructura

1.3.1.1.1.2	**Obtener el costo de inversión del nuevo equipamiento.**
Descripción	Se establece los costos del nuevo equipamiento sugerido para operar en la entidad financiera.
Actividades	• Establecer lista de vendedores calificados para solicitar el RFI. • Establecer el proveedor • Realizar un reporte ejecutivo para presentar a la dirección de informática
Duración	3 días.
Responsable	Administrador del proyecto.

1.3.1.1.1.2.1	**Obtener aprobación de la dirección de informática.**
Descripción	Se establece una reunión de directorio para presentar el análisis del costo beneficio para la adquisición del nuevo equipamiento sugerido.
Actividades	• Establecer canal de comunicaciones. (Por email, carta, teléfono) • Definición de la fecha y hora de la reunión de directorio. • Establecer los participantes y el expositor para sustentar el nuevo equipamiento sugerido.
Duración	5 días.
Responsable	Administrador del proyecto.

1.4	**Seguridad Perimetral.**
Descripción	Se estiman todas las buenas prácticas de seguridad lógica establecidas en el ISO 27001
Actividades	• Determinar el alcance de la seguridad perimetral. • Establecer políticas de confidencialidad de la información. • Establecer policitas de la seguridad de la información. • Instruir al personal técnico sobre las políticas de seguridad de la información.
Duración	22 días.
Responsable	Seguridad de la información.

1.4.1	**Obtener diagrama de Red corporativo.**
Descripción	Obtener o generar un diagrama en MS Visio la red corporativa de la entidad bancaria.
Actividades	• Documentar toda la información de red de las estaciones de trabajo • Documentar la información de la DMZ de los servidores en producción. • Establecer un diseño de direccionamiento IP en cada sucursal y agencias
Duración	1 día
Responsable	Ing. en Infraestructura.

1.4.1.1	**Determinar equipo de seguridad perimetral.**
Descripción	Se realiza un análisis de los equipos de seguridad en el mercado para establecer la marca y modelo que se ajusta a las necesidades de la entidad bancaria.
Actividades	• Investigar las especificaciones técnicas de los equipos de seguridad perimetral. • Determinar el costo del equipo de seguridad perimetral. • Determinar los tipos incidentes que mitiga la herramienta.
Duración	1 día.
Responsable	Ing. en Infraestructura y Seguridad de Información.

1.4.1.1.1	**Implementación de equipo de seguridad perimetral.**
Descripción	Se estable los parámetros de configuración que debe tener para proceder a la instalación del equipo de seguridad perimetral. No se implementa. Solo de establece los parámetros de configuración.
Actividades	• Establecer el modo de operación del equipo de seguridad lógica. Puede ser en L2 (Sniffer) o L3 (Firewall) • Determinar las ventajas y desventajas de cada modo de operación. • Configuración de reportes de los incidentes mitigados.
Duración	10 días
Responsable	Ing. en Infraestructura y Seguridad de la información.

1.4.1.1.2	**Reporte de incidentes de seguridad encontrados.**
Descripción	Se establece los periodos que se generan los reportes de incidentes de seguridad encontrados y mitigados.
Actividades	• Establecer el tipo de archivo a generar. (doc, PDF, HTML, Etc) • Establecer los destinatarios del reporte.
Duración	10 días.
Responsable	Seguridad de la información.

1.5	**Contingencia en equipos de Telecomunicaciones.**
Descripción	Se realiza un modelo eficiente para la contingencia de los servicios de telecomunicaciones como internet y transmisión de datos.
Actividades	• Establecer el alcance de la contingencia para los servicios de telecomunicaciones.
Duración	11 días.
Responsable	Ing. en Telecomunicaciones.

1.5.1	**Definir empresa de Telecomunicaciones.**
Descripción	Se define en base a los requerimientos solicitados la empresa de telecomunicaciones que prestaran el servicio para el banco.
Actividades	• Desarrollar el RFI a las empresas con mayor cobertura en el Ecuador. • Solicitar la cobertura. • Determinar precio por Kbps. • Solicitar pruebas de servicio y certificaciones de calidad. • Definición de proveedor principal y de respaldo.
Duración	1 día.
Responsable	Ing. en Telecomunicaciones.

1.5.1.1	**Determinar número de enlaces redundantes por agencia.**
Descripción	Se realiza un estudio para determinar la cantidad de enlaces por agencia que debe tener la entidad bancaria.
Actividades	• Verificar el tipo de última milla (Radio, Fibra Óptica) que tendrían cada agencia y sucursal bancaria. • Determinar el costo del servicio para implementación de contingencia.
Duración	2 días.
Responsable	Documentador Líder.

1.5.1.2	**Determinar si contemplan SLA**
Descripción	Se solicita que la empresa de telecomunicaciones envié periódicamente un reporte con el SLA.
Actividades	• Establecer el % del SLA (Acuerdo de nivel de servicio) • Establecer penalizaciones. • Establecer con el proveedor de telecomunicaciones el envío del SLA por cada mes del año.
Duración	1 día.
Responsable	Ing. en Telecomunicaciones.

1.5.1.2.1	**Determinar costo mensual por cada enlace.**
Descripción	Se establece con el proveedor de telecomunicaciones el precio instalación de última milla principal o de respaldo.
Actividades	• Calcular el precio que debería desembolsar la entidad financiera cada mes. • Establecer el número de enlaces principales y de respaldo.
Duración	1 día.
Responsable	Administrador del proyecto.

1.5.1.1.1	**Determinar protocolo de enrutamiento.**
Descripción	Se establece el protocolo de enrutamiento para la implementación del respaldo automático.
Actividades	• Determinar protocolo que realice la conmutación automática hacia el enlace de respaldo. • Determinar el equipo de telecomunicaciones para realizar la contingencia automática.
Duración	1 día.
Responsable	Ing. en Telecomunicaciones.

1.5.1.1.1.1	**Implementar protocolo de enrutamiento.**
Descripción	Se planifica la hora y fecha de las configuraciones a nivel de capa 3 para la implementación del respaldo automático.
Actividades	• Establecer las configuraciones de IP del protocolo. • Establecer con el proveedor de telecomunicaciones una VLAN independiente para el tráfico de datos. • Se programa una ventana de trabajo con el proveedor de telecomunicaciones para no afectar el flujo de trabajo diario en la entidad bancaria.
Duración	2 días.
Responsable	Ing. en Telecomunicaciones.

1.5.1.1.1.1.1	**Pruebas de conmutación automática.**
Descripción	Se define las pruebas de conmutación automática del enlace principal al enlace de respaldo.
Actividades	• Definir la fecha y hora de las pruebas. • Confirmar que se está utilizando el enlace de respaldo. • Verificar que todos los sistemas estén operativos con el enlace de respaldo. • Verificar que se vuelve a conmutar al enlace principal. • Guardar las configuraciones de los equipos de red.
Duración	1 días.
Responsable	Ing. en Telecomunicaciones.

1.5.1.1.1.1.1.1	**Documentar resultados de las pruebas realizadas.**
Descripción	Se documenta todo hallazgo y oportunidad de mejora de las pruebas realizadas con el proveedor de telecomunicaciones.
Actividades	• Documentar las IPs de salida de los enlaces principales. • Documentar las IPs de salida al realizar la conmutación automática. • Establecer el tiempo de conmutación del protocolo de enrutamiento. • Documentar fallas en la implementación. • Establecer oportunidades de mejora y conclusiones.
Duración	1 día.
Responsable	Documentador Líder.

1.6	**Contingencia de Sistemas.**
Descripción	Se estudia los diferentes métodos y configuraciones para la contingencia de los sistemas informáticos del Banco.
Actividades	• Se establece las aplicaciones críticas de la entidad financiera para proceder a la implementación del respaldo.
Duración	55 días.
Responsable	Ing. en Sistemas.

1.6.1	**Implementación de replica automática de bases de datos.**
Descripción	Se determina la fecha y hora de la implementación de la réplica de la base de datos. Adicional la configuración necesaria para dejar en producción la réplica automática.
Actividades	• Establecer el procedimiento para la implementación de la réplica. • Establecer el tamaño en bytes de la base de datos. • Probar la contingencia automática. • Documentar resultados.
Duración	15 días.
Responsable	Ing. en Sistemas.

1.6.2	**Implementación de automatización de respaldo de aplicaciones.**
Descripción	Se establece la fecha y hora para la implementación de respaldo para aplicaciones bancarias.
Actividades	• Establecer las configuraciones necesarias para la automatización de respaldo en las aplicaciones. • Comprobar que los respaldos cumplen con las normas de seguridad establecidas por el Sans Institute. • Reportar los resultados de la verificación de las normas de seguridad lógica. • Documentar las pruebas realizadas.
Duración	5 días.
Responsable	Ing. en Sistemas.

1.6.2.1	**Implementación de discos Raid.**
Descripción	Se establece la configuración del arreglo de discos.
Actividades	• Establecer el tipo de Raid a implementar. • Determinar ventajas y desventajas de la implementación. • Establecer procedimiento para la implementación Raid.
Duración	15 días.
Responsable	Ing. en Sistemas

1.6.2.2	**Implementación de contingencia física (Datacenter externo)**
Descripción	Se realizar las gestiones necesarias para obtener un datacenter externo por exigencia de la norma del BCP.
Actividades	• Cotizar el servicio de datacenter externo. • Establecer si es conveniente arrendar un espacio en el datacenter o adquirir metros cuadrados en el mismo. • Determinar el costo de la implementación. • Aprobar el recurso financiero para la implementación del datacenter.
Duración	20 días.
Responsable	Ing. en Sistemas.

1.7	**Elaboración de BCP para sistemas informáticos y telecomunicaciones.**
Descripción	Se realizar la documentación del alcance del BCP para su posterior implementación.
Actividades	• Establecer los procedimientos para la implementación del BCP. • Realizar simulaciones para verificar la efectividad del BCP. • Realizar manuales de procedimientos para activar el BCP.
Duración	20 días.
Responsable	Experto BCP

1.7.1	**Identificar los activos de información.**
Descripción	Se realiza un estudio de los sistemas de información de la entidad bancaria. También los servicios críticos para poder operar con normalidad.
Actividades	• Establecer reuniones con los administradores de los servicios críticos de la organización. • Determinar los servicios y asignarle un grado de prioridad. • Determinar cuáles servicios se contempla en el BCP y cuales se acepta el riesgo.
Duración	2 días.
Responsable	Ing. en Sistemas.

1.7.1.1	**Recolectar información de los procesos informáticos.**
Descripción	Determinar la información critica que es imprescindible para obtener la continuidad del negocio.
Actividades	• Realizar reuniones periódicas para recolectar información de los procesos internos de la entidad bancaria. • Realizar un reporte en el que se indique los resultados de las reuniones establecidas.
Duración	3 días.
Responsable	Documentador Líder.

1.7.1.1.1	**Diseñar el plan de contingencia.**
Descripción	Se genera la documentación del plan de contingencia para los sistemas informáticos y de telecomunicaciones.
Actividades	• Se establece las mejoras prácticas del BCP. • Difundir la información para que cada miembro sepa los procedimientos a realizar en caso de activar el BCP. • Realizar un calendario para simulaciones del BCP.
Duración	15 días.
Responsable	Experto BCP.

1.8	**Plan de Mantenimiento Preventivo.**
Descripción	Se genera documentación para el plan de mantenimiento preventivo de los equipos adquiridos.
Actividades	• Definir los aspectos ambientales que estipula el fabricante de los equipos. • Determinar la existencia de un departamento de mantenimiento en la entidad financiera. • Verificar si existen políticas de mantenimiento periódico en los sistemas de producción y equipos de telecomunicaciones.
Duración	35 días.
Responsable	Experto BCP

1.8.1	**Cronograma de Mantenimiento Preventivo.**
Descripción	Se establece la fecha y hora de los mantenimientos según lo que indique el fabricante del producto.
Actividades	• Asignación del responsable del mantenimiento del equipo. • Establecer los equipos que estarán en cronograma de mantenimiento • Realizar el formato de acta de finalización de mantenimiento. • Establecer la periodicidad del mantenimiento según las especificaciones del fabricante.
Duración	5 días.
Responsable	Administrador del Proyecto.

1.8.1.1 / 18.1.2	**Plan de Mantenimiento preventivo para Telecomunicaciones y de servidores**
Descripción	Se realiza la planificación del mantenimiento preventivo de los equipos de telecomunicaciones y las últimas millas pertenecientes al proveedor.
Actividades	• Realizar gestiones con el proveedor de telecomunicaciones para que presente la planificación de mantenimiento de las últimas millas que ingresan a las agencias y sucursales de la entidad bancaria. • Planificar el mantenimiento de los CPEs de cada agencia y sucursal. • Planificar el mantenimiento preventivo para servidores en producción.
Duración	15 días cada uno.
Responsable	Ing. en Sistemas e Ing. en Infraestructura.

Cuadro 6. Diccionario EDT.
Elaborado por: Autores

5.2.1.3 Lista de actividades.

La lista de actividades comprende el nombre de todas las tareas y la asignación del recurso humano que será encargado de completar la misma.

Anexo [3]. Lista de Actividades

5.2.2 Diagrama de Red.

En el siguiente anexo tenemos la representación grafica de las actividades del cronograma del proyecto. Aquí podemos observar las dependencias de las tareas.

Anexo [4]. Diagrama de red

5.2.3 Determinar Camino Crítico.

Aquí se determina las tareas con mayor duración. Un retraso en estas actividades genera un gran impacto negativo en el proyecto.

Anexo.[5] Camino critico EDT

5.2.4 Desarrollar Cronograma.

Con el diagrama de Gantt buscamos establecer la representación grafica de las tareas y el tiempo asignado para completar el proyecto.

Anexo [6]. Diagrama de Gantt

5.2.5 Desarrollar Presupuesto

Para la realización de este proyecto se ha planteado un presupuesto que se debe respetar, a continuación se detalla de qué manera se prevé costear la utilización de recursos a lo largo del proyecto, estos costos pueden variar de

alguna manera pero el impacto en caso de que suceda no debe afectar significativamente al proyecto. El valor del presupuesto detallado a continuación es por el tiempo de duración del proyecto.

Presupuesto del Proyecto por Recurso Humano

Cargo	Nombre del recurso	Capacidad máxima	Tasa estándar
Ing. en Telecomunicaciones	Fernanda Gutiérrez	100%	$ 6,25/hora
Ing en Infraestructura	Sebastián Cordero	100%	$ 6,25/hora
In. en Sistemas	Diana López	100%	$ 6,25/hora
Documentador Líder	Claudia Núñez	100%	$ 5,00/hora
Documentador	Sergio Villa	100%	$ 3,13/hora
Seguridad De Información	Juan Aguirre	100%	$ 6,25/hora
Documentador	Xavier Castellano	100%	$ 3,13/hora
Administrador del Proyecto	Alberto Guevara	100%	$ 7,50/hora
BCP	Pablo Sánchez	100%	$ 6,25/hora
Analista auxiliar	Julia Merino	100%	$ 3,75/hora
Analista de Sistemas	Álvaro Gonzalez	100%	$ 5,00/hora

Cuadro 7: Presupuesto de Recursos Humanos
Elaborado por: Autores
Anexo [7]. Presupuesto

5.2.6 Plan de Calidad

Adquisición del equipamiento: Realizaremos la compra de equipos de reconocida marca para levantar nuestro modelo de contingencia. Analizaremos los proveedores para la selección de los mejores en el mercado y que cumplan con las fechas de entrega.

Ajustamiento del modelo a la realidad de la entidad bancaria: Antes de implementar el modelo verificaremos con la dirección de informática si se ajusta a la realidad de la entidad bancaria.

Aseguramiento de la calidad:

- Utilizar los controles críticos de seguridad recomendados por el "SANS INSTITUTE".
- Utilizar equipos de telecomunicaciones CISCO los cuales son reconocidos por su calidad de servicio.

Control de la calidad:

- Utilización de un consultor externo experto en Ethical Hacking para que realice pruebas del modelo implementado
- Se realizarán simulacros teniendo como base el plan de Contingencia frente a incidentes que atenten contra el flujo de trabajo de la empresa en donde se controlara que no se vea afectada ninguna área de la institución bancaria

5.2.6.1Determinar estándares de calidad.

En vista de la necesidad de asegurar la buena ejecución de nuestras tareas se han seleccionado estándares que se adaptan a la finalidad de nuestro proyecto, es por esto que se tomarán como base para su desarrollo.

SANS Institute: Esta institución posee una gran base de datos basado en su experiencia en numerosos campos como seguridad de redes, análisis forense, la auditoría, el liderazgo de la seguridad y la seguridad de las aplicaciones.

ISO 27001, especificación del sistema de gestión de la seguridad de la información (SGSI). Esta norma será certificable bajo los esquemas nacionales de cada país.

ISO 27002, actualmente la ISO 17799, que describe el Código de buenas prácticas para la gestión de la seguridad de la información.

BS 25999: La norma ayuda a establecer las bases de un sistema BCM (Business Continuity Managment) y se ha concebido para mantener en marcha las actividades durante las circunstancias más inesperadas y desafiantes: protege a los empleados, su reputación y proporciona la capacidad de continuar con la actividad y el comercio.

5.2.6.2 Métricas de medición.

Se ha seleccionado los siguientes controles para asegurar que el modelo de contingencia sea exitoso.

Numero de controles Implementados de SANS INSTITUTE / Total de controles de SANS INSTITUTE

Medición: Trimestral

- Total de Vulnerabilidades Mitigadas / Total de Vulnerabilidades encontradas

Medición: Semanal

- Número de incidentes de seguridad mitigados / Total de Incidentes de seguridad reportados.

Medición: Semanal

- Acciones correctivas implementadas / Acciones correctivas planificadas

Medición: Semanal

- Simulacro de contingencias exitosas/ Total de simulacros realizados

5.2.6.3Programa de Calidad

Adquisición del equipamiento: Realizaremos la compra de equipos de reconocida marca para levantar nuestro modelo de contingencia. Analizaremos los proveedores para la selección de los mejores en el mercado y que cumplan con las fechas de entrega.

Ajustamiento del modelo a la realidad de la entidad bancaria: Antes de implementar el modelo verificaremos con la dirección de informática si se ajusta a la realidad de la entidad bancaria.

Aseguramiento de la calidad:

Utilizar los controles críticos de seguridad recomendados por el “SANS INSTITUTE”

Utilizar equipos de telecomunicaciones CISCO los cuales son reconocidos por su calidad de servicio.

Control de la calidad:

Utilización de un consultor externo experto en Ethical Hacking para que realice pruebas del modelo implementado.

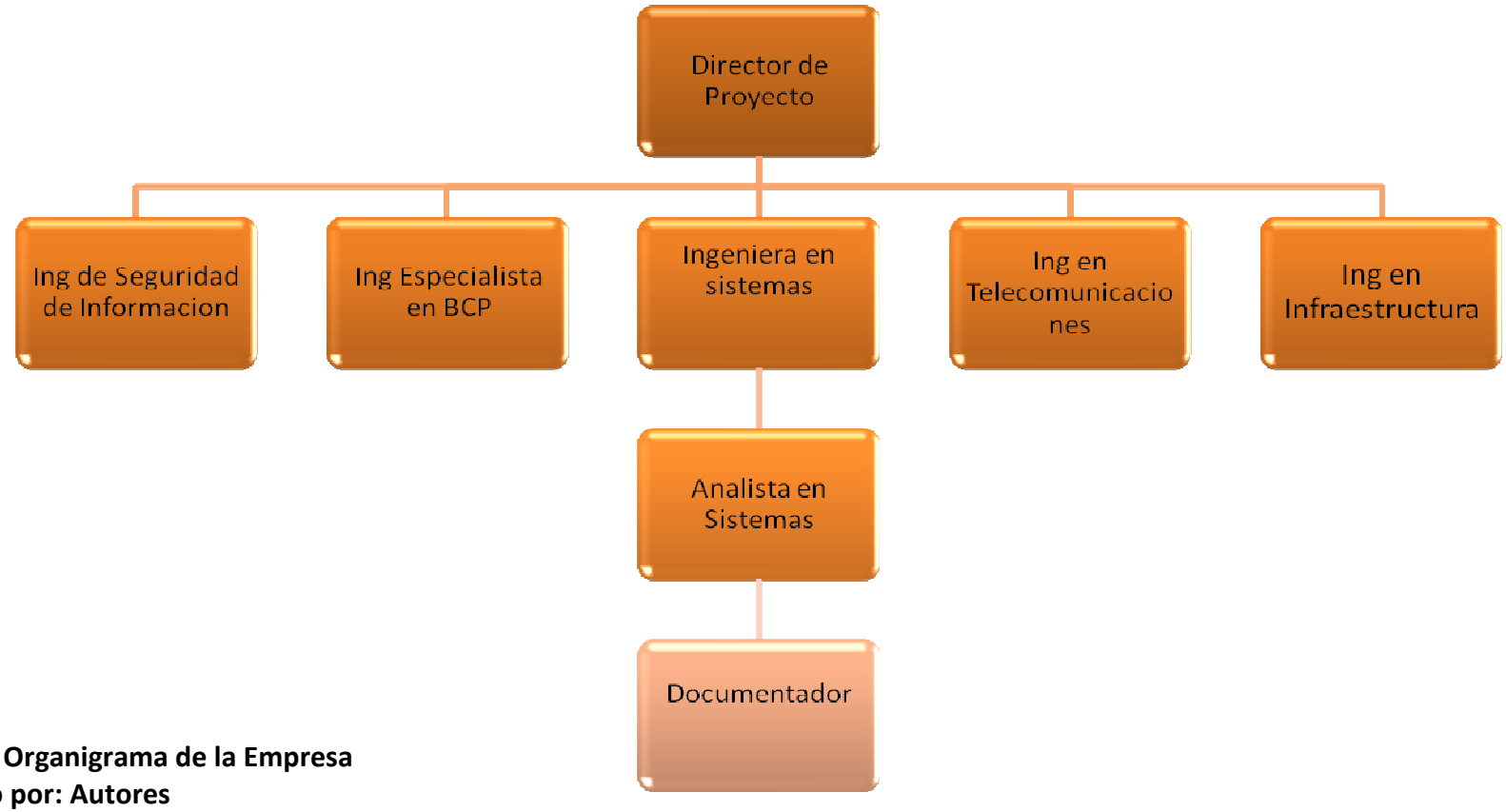
Se realizarán simulacros teniendo como base el plan de Contingencia frente a incidentes que atenten contra el flujo de trabajo de la empresa en donde se controlara que no se vea afectada ninguna área de la institución bancaria.

5.2.7 Plan de Recursos Humanos.

5.2.7.1 Determinar Roles y responsabilidades.

Cada miembro del equipo de trabajo tiene roles específicos que nos ayudaran a cumplir todas las tareas establecidas en cronograma de trabajo.

5.2.7.2Organigrama del Proyecto



Cuadro 8. Organigrama de la Empresa
Elaborado por: Autores

5.2.7.3Tabla de Asignación de Tareas

Descripción Tarea	Asignaciones
Diseñar un modelo de Contingencia de Sistemas y Telecomunicaciones para Entidades Bancarias del Ecuador	
Reporte de Vulnerabilidades encontradas en sistemas bancarios	
Levantamiento de información de sistemas existentes	Claudia Núñez Xavier Castellano Sergio Villa
Escanear Vulnerabilidades del sistema	Diana López Julia Merino Álvaro Gonzales
Documentar Vulnerabilidades encontradas	Claudia Núñez Sergio Villa
Análisis de Impacto que causaría las vulnerabilidades encontradas	Diana López Álvaro Gonzales
Análisis de Costo / Beneficio del nuevo equipamiento sugerido	
Recolección de volumen de transacciones diarias	Xavier Castellano Sergio Villa
Proyección de Volumen en 5 años	Alberto Guevara
Realizar Benchmark	Alberto Guevara
Justificar la adquisición del nuevo equipamiento	Sebastián Cordero
Obtener el costo de inversión del nuevo equipamiento	Sebastián Cordero Alberto Guevara
Obtener aprobación de la dirección de Informática	Alberto Guevara
Seguridad Perimetral	
Obtener diagrama de red corporativo	Fernanda Gutiérrez
Determinar equipo de seguridad perimetral	Sebastián Cordero
Implementación de equipo de seguridad perimetral	Sebastián Cordero Juan Aguirre
Reporte de incidentes de seguridad encontrados	Claudia Núñez Sebastián Cordero Juan Aguirre

Descripción Tarea	Asignaciones
Contingencia en equipos de telecomunicaciones	
Definir empresa de telecomunicaciones	Fernanda Gutiérrez
Determinar numero de enlaces redundantes por agencia	Claudia Núñez Sergio Villa
Determinar protocolo de enrutamiento	Fernanda Gutiérrez
Implementar protocolo de enrutamiento	Fernanda Gutiérrez
Pruebas de Conmutación Automática	Fernanda Gutiérrez Juan Aguirre
Documentar resultados de las pruebas realizadas	Xavier Castellano
Determinar si contemplan SLA	Fernanda Gutiérrez
Determinar costo mensual por cada enlace	Sebastián Cordero Alberto Guevara
Contingencia de sistemas	
Implementación de replica automática de bases de datos	Diana López Julia Merino Álvaro Gonzales
Implementación de Automatización de respaldo de aplicaciones	Diana López Álvaro Gonzales
implementación de discos raid	Diana López
Implementación de contingencia física (datacenter externo)	Diana López Sebastián Cordero
Elaboración de BCP para sistemas informáticos y telecomunicaciones	
Identificar activos de información	Fernanda Gutiérrez
Recolectar información de los procesos informáticos	Claudia Núñez Xavier Castellano
Diseñar el plan de contingencia	Pablo Sánchez Diana López Fernanda Gutiérrez
Plan de Mantenimiento Preventivo	
Cronograma de Mantenimiento Preventivo	Alberto Guevara
Plan de mantenimiento preventivo para telecomunicaciones	Fernanda Gutiérrez
Plan de mantenimiento preventivo para servidores	Sebastián Cordero Diana López

Cuadro 9. Lista de Tareas Asignadas al Personal
Elaborado por: Autores

5.2.8 Plan de Comunicaciones

5.2.8.1 Políticas de Comunicación:

Se realizará la convocatoria de reuniones a las personas interesadas, al final de la misma se procederá a la elaboración de la minuta y se informara a todos los convocados con los temas tratados y conclusiones hechas

Se debe llevar un registro de asistencia a las reuniones, con la firma de los participantes.

Se planificaran reuniones en cada inicio de proyecto, en donde se pongan en claro los objetivos a alcanzar en conjunto con el equipo de trabajo

Deben convocarse a reuniones de solución de problemas en caso de ser necesarias.

Se crearan reuniones para revisiones semanales de la situación actual del proyecto en construcción. La convocatoria la realizará el administrador del Proyecto.

Se concretaran una reunión para el diseño técnico del proyecto con el quipo de trabajo y el administrador del proyecto.

Se organizaran reuniones periódicas de avance de proyecto en donde se mostrara al cliente y patrocinadores los entregables terminados

Debe realizarse las reuniones de cierre de proyecto en donde el administrador del proyecto muestre el producto final al cliente y al patrocinador para su respectiva aprobación final.

Los informes de avances se realizarán a lo largo de la implementación y serán distribuidos a los interesados.

Se emitirá un informe final con las características y procesos implicados en la creación del proyecto y se distribuirá a los interesados.

5.2.8.2 Objetivos del Plan de Comunicaciones:

- Mantener al personal informado de los cambios de administrador del proyecto
- Definir las metas y objetivos para que el equipo de trabajo tenga claro lo que se realizará durante el proyecto.

El envío y la recepción de mensajes se realizarán en las siguientes etapas del proyecto:

- De Inicio de proyecto (metas, objetivos, alcance)
- Continuidad y avance del proyecto (presentación de resultados fases del proyecto)
- Cierre del proyecto (presentación del proyecto)
- Grupos Involucrados previamente definidos
- Directiva General
- Administrador del proyecto
- Equipo de trabajo
- Patrocinador y Cliente final

5.2.8.3 Tecnologías o medios a emplear para comunicarse

- Juntas de trabajo
- Emails
- Convocatorias vía Outlook
- Teléfono
- Intranet
- Programa de Comunicación
- Junta de Inicio de proyecto
- Reuniones semanales de avance (equipo de trabajo y administrador de proyecto)
- Reunión de revisión de avances con usuario final (administrador de proyecto y usuario final)
- Junta de cambios solicitados por el usuario (equipo de trabajo y administración de proyecto)
- Cierre del proyecto

5.2.8.4 Periodos y Programación de Reuniones

INVOLUCRADO	QUE COMUNICAR	CUANDO COMUNICAR	A QUIENES COMUNICAR	FORMATO	RESPONSABLE
Director de Proyecto	Inicio de Proyecto	una vez por proyecto	Patrocinador, Stakeholders Equipo de Trabajo	Correo Electrónico	Director del Proyecto
Director del Proyecto	Avances de Proyecto	cuatro veces por mes	Equipo de Trabajo	Circular / Correo electrónico	Equipo de Trabajo / Responsable del entregable
Director del Proyecto	Avances del Proyecto	dos veces por proyecto	Patrocinador	Correo Electrónico	Director del Proyecto
Patrocinador	Solicitudes de Cambios	a demanda	Director del proyecto	Carta en sobre cerrado	Patrocinador

INVOLUCRADO	QUE COMUNICAR	CUANDO COMUNICAR	A QUIENES COMUNICAR	FORMATO	RESPONSABLE
Director del Proyecto	Cierre del proyecto	Fin del proyecto	Patrocinador Stakeholders	Circular/ Correo Electrónico	Director del Proyecto
Director del Proyecto	Feedback y lecciones aprendidas	Fin del proyecto	Equipo de Trabajo	Circular	Director del Proyecto

Cuadro 10. Matriz de Periocidad de Reuniones
Elaborado por: Autores

5.2.9 Plan de Riesgos

5.2.9.1 Identificación de Riesgos

Categoría	Riesgo	Evento Disparador	Acciones Preventivas	Acciones Correctivas	Responsable
Seguridad Lógica	No tengan documentación de Red implementada	No tengan diagrama de red	Solicitar el documento antes de empezar con el entregable de Seguridad lógica	El Ing. de seguridad lógica y un documentador serán responsables del levantamiento de información de la red corporativa	Ing. de seguridad lógica

Categoría	Riesgo	Evento Disparador	Acciones Preventivas	Acciones Correctivas	Responsable
Seguridad Lógica	Nueva vulnerabilidad en los sistemas bancarios	Incidente de seguridad reportado	Estar actualizado con las ultimas vulnerabilidades según el Instituto Sans	Mitigación del riesgo o eliminación del riesgo con los equipos de seguridad perimetral	Encargado de la seguridad de la información
Hardware	Daño de servidores de computo	Daño de un componente del servidor	Solicitar garantía y tiempos de soporte ante un incidente	Monitoreo de rendimiento de los servidores	Infraestructura
Hardware	Condiciones eléctricas defectuosas	Bajo rendimiento de los servidores de Producción	Verificar las conexiones eléctricas alineadas a la norma	Colocar UPS y reguladores en el Centro de computo	Infraestructura

Categoría	Riesgo	Evento Disparador	Acciones Preventivas	Acciones Correctivas	Responsable
Adquisición de equipamiento	Retraso en entrega de equipos	Línea Base, retraso de actividades por falta de equipo	Penalizaciones al proveedor de equipos.	Trasladar el riesgo al proveedor	Administrador del proyecto

Cuadro 11.Identificacion de Riesgo
Elaborado por: Autores

5.2.9.2Cualificación de Riesgo.

Categoría	Riesgo	Probabilidad de ocurrencia	Impacto potencial
Seguridad Lógica	No tengan documentación de Red implementada	A	M
Equipos de Telecomunicaciones	Equipos Defectuoso	B	A
Equipos de Telecomunicaciones	Mala funcionalidad de equipos Cisco	M	B
Presupuesto	No sea aprobado el presupuesto para nuevo equipamiento	A	A

Tipo	Categoría
A	Alto
M	Medio
B	Bajo

Categoría	Riesgo	Probabilidad de ocurrencia	Impacto potencial
Contingencia	No tener éxito en las pruebas de contingencia de Telecomunicaciones	M	A
Seguridad Lógica	Nueva vulnerabilidad en los sistemas bancarios	M	A
Hardware	Daño de servidores de computo	B	A
Hardware	Condiciones eléctricas defectuosas	B	B
Adquisición de equipamiento	Retraso en entrega de equipos	M	A

Cuadro 12. Cualificación de Riesgo
Elaborado por: Autores

5.2.10 Plan de Adquisiciones

5.2.10.1 Políticas de Adquisiciones.

La creación de una lista de proveedores con calificaciones previas según los servicios prestados y experiencias

Los proveedores que no hayan brindado un buen servicio constaran en una lista negra de proveedores con el motivo del por qué se encuentran ahí

El departamento solicitante de recursos a comprar o contratar debe enviar al Dpto. de Compras y Adquisiciones un RFP (Request For Proposal) para solicitar propuestas de posibles vendedores de productos o servicios con las especificaciones necesarias para la compra del servicio o producto

Los proveedores deben enviar la información o RFI (Request for Information) donde el proveedor m

Las solicitudes de nuevos recursos deben ser aprobadas por el jefe del proyecto o el administrador

Las servicios seleccionados como mejores deben ser consultados por el solicitante y el dpto de compras para escoger al que ofrece el mejor servicio

5.2.10.2 Objetivos del Plan de Adquisiciones.

Cubrir las necesidades en materia de equipos, software, productos o servicios necesarios para la creación del proyecto en su totalidad

Contratar los recursos humanos solicitados para su respectiva participación en el proyecto

Seleccionar la mejor opción de los recursos necesarios para su utilización y optimo desempeño

5.2.10.3 Tipos de Contratos a emplear

Tiempo y Materiales: Utilizaremos este tipo de contrato ya que las contrataciones externas que tendremos son consultores que necesitan materiales a medida que se realizan los estudios solicitados.

Costo Fijo: Este tipo de contrato nos servirá para la adquisición de software de vulnerabilidades necesario para la ejecución del proyecto

5.2.10.4 Condiciones para solicitar la inscripción como proveedor.

Acreditar una antigüedad de 3 años o más, como comerciante, mediante el registro mercantil (Certificado de Cámara de Comercio);

Demostrar experiencia como Proveedor de bienes o servicios, importador, fabricante o distribuidor exclusivo, conforme al Certificado de Experiencia.

Garantizar la existencia de stocks o inventarios de los bienes que ofrece o suministra o su disposición, conforme a la Solicitud de Inscripción.

No estar condenado en procesos penales

5.2.10.5 Requisitos documentales para solicitar la inscripción como proveedor.

- Copia del Registro Único Tributario (RUT);
- Certificado de existencia y representación legal cuya fecha de expedición no sea superior a un (1) mes, si el aspirante a Proveedor

es persona jurídica; si es persona natural, certificado de Matrícula Mercantil con fecha de expedición no superior a un (1) mes;

- Copia del documento de identificación del Representante Legal, si es persona jurídica; si es persona natural, de la cédula del Proveedor;
- Acreditación de experiencia, mediante tres (3) certificaciones comerciales expedidas por clientes del Proveedor y diligenciar el Certificado de Experiencia.
- Certificación bancaria sobre cuenta vigente, que contenga el nombre del titular, tipo de cuenta y número de la misma, expedida con antigüedad no mayor a tres (3) meses, a la fecha de su presentación para solicitar el registro;
- OPCIONAL: Certificado de norma ISO, OHSAS u otra norma, si el Proveedor cuenta con los procesos respectivos.
- OPCIONAL: Entrega de portafolio de servicios, si el Proveedor cuenta con el mismo.

Conclusiones y Recomendaciones

Se concluye que las entidades financieras deben estar en constante mejora de los servicios en línea para disminuir el gasto operativo que tienen las sucursales y agencias bancarias. Esto conlleva a invertir en seguridad lógica en los sistemas de información. Tener información confidencial de los clientes genera que la gerencia de informática este en constante actualización de las vulnerabilidades que existe en la red de datos.

La falta de leyes o normas que regulen el funcionamiento de los equipos de sistemas y telecomunicaciones permite que exista cierto desconocimiento por parte de las entidades, y esto aumenta el riesgo al no tomar las medidas adecuadas de preservar la seguridad de información. Adicionalmente existen restricciones al momento de proveer datos necesarios para el análisis.

Referencias

[1] Jean-Marc Royer. Seguridad en la informática de Empresa. Barcelona: Editions, Agosto 2004

[2] Carlos Araya Pacheco, “Administración de los riesgos en los sistemas de información como herramienta de gestión para administradores”. Universidad Católica del Norte, Ciudad de Antofagasta, Chile.

[3]http://www.sans.org/ Sans Institute buenas prácticas sobre la seguridad de información sobre redes y aplicaciones

[4] Roberto Muñoz Bermeo. Análisis Du Pont del sistema financiero del Ecuador: Superintendencia de Bancos y seguros del Ecuador

TÍTULO:		
Acta de constitución del proyecto		
CÓDIGO	**FECHA**	**REVISIÓN**
AC001	22/08/2012	

REALIZADO POR	FECHA	FIRMA
Representante de Patrocionio	22/08/2012	

1. INFORMACIÓN GENERAL

Enunciado del proyecto:	Diseñar un modelo de contingencia de sistemas y telecomunicaciones para las Entidades bancarias del Ecuador	***ID del proyecto:***	AC001
Sponsor:	Banco Guayaquil	***Representante del sponsor:***	Representante de patrocinio

2. JUSTIFICACIÓN DEL PROYECTO

Todos los sistemas están propensos a fallos ya sea por algún ataque externo o daño que hardware o software. Algunos de estos fallos toman días y hasta semanas generando inconformidad en los clientes. No existe un análisis de las incidencias que pueden ocurrir y peor aun estar prevenidos

Adicional los Gerentes generales las instituciones bancarias necesitan tener los sistemas informáticos como los sitios web para realizar las transacciones en línea, de esta manera tratar de equilibrar el tránsito de los clientes con el objetivo de minimizar el costo de operación de las sucursales.

Los constantes ataques a diversas entidades públicas y privadas son cada día más frecuentes en nuestro país.

En nuestro caso las entidades bancarias son objetivos principales de los hackers que prueban las vulnerabilidades de los sistemas informáticos.

Una de las razones es que el recurso del internet es inseguro y tanto el usuario como el banquero tienen temor en utilizar estas herramientas informáticas pero con un estudio de vulnerabilidad y contingencias se podrá recuperar durante una falla en los sistemas.

. Otro recurso muy importante es la disponibilidad de la salida al internet otorgado por el proveedor de telecomunicaciones. Los servidores Web deben estar operativos las 24 horas los 365 días del año y si un proveedor sufre alguna caída la entidad bancaria debe tener un plan de contingencia para re direccionar el trafico a otro proveedor. Es necesario hacer un correcto análisis de los proveedores de internet y datos en el Ecuador y así minimizar el impacto por la falla de este agente externo.

1.1 OBJETIVOS DEL NEGOCIO

Diseñar un plan adecuado y real con los activos necesarios para asegurar el funcionamiento del modelo de negocios y la operatividad en las Entidades Bancarias ante cualquier incidente relacionado a sistemas y telecomunicaciones.

1.2 OBJETIVOS ESPECÍFICOS.

- Identificar los principales problemas que afectan a las áreas de sistemas y telecomunicaciones
- Diseñar y estructurar el mejor plan de contingencia para las Entidades Bancarias
- Dar a conocer al personal encargado del Plan de Contingencia las principales vulnerabilidades que afectan al área de sistemas y redes de estas entidades.
- Identificar los recursos mínimos con los que debe contar la institución bancaria

3. DESCRIPCIÓN DEL PROYECTO

1.3 DESCRIPCIÓN DEL PROYECTO

Nuestro proyecto consiste en realizar un modelo de contingencias para sistemas informáticos bancarios ecuatorianos. Es necesario que la entidad bancaria siga sus operaciones diarias durante un incidente de seguridad. Realizaremos un estudio de las vulnerabilidades existentes con respecto a los equipos informáticos como los de telecomunicaciones. Para los servicios de transmisión de datos entre agencias seleccionaremos el mejor modelo de contingencia por cualquier falla de los proveedores de telecomunicaciones.

4. REQUERIMIENTOS DEL PROYECTO/ENTREGABLES

- Análisis de las posibles contingencias para sistemas informáticos y equipos de telecomunicaciones, en el cual se de a conocer detalladamente las características necesarias para preveer posibles ataques contra la infraestructura de la entidad financiera

- Elaborar el Bcp con un alcance establecido de sistemas y telecomunicaciones

- Analizar la infraestructura de las 5 entidades financieras más importantes en el medio, para elaborar un plan de mejora general frente a los equipos de sistemas y telecomunicaciones

5. HITOS Y ENTREGABLES DE LA GESTIÓN DE PROYECTOS

El levantamiento de información nos servirá como retroalimentación para el análisis y mejora de los equipos, esto se conseguirá por medio de las visitas a bancos como consultoría de seguridades a su favor lo cual nos permitía realizar un inventario de tecnología a adquirida por los sistemas bancarios

Informe de nuevas tecnologías de seguridad adaptables al sistema bancario, en el cual se especifican las plataformas y herramientas que servirán para disminuir los frecuentes ataques informáticos y huecos de seguridad en el sistema. Además de nueva infraestructura a nivel de comunicación de datos

Informe de condiciones generales de seguridad que deben brindar los proveedores de internet y comunicación de datos frente a los sistemas bancarios, para proveer un sistema optimo con contingencias físicas y lógicas.

Análisis de costo / beneficio de las diferentes empresas de telecomunicaciones del Ecuador

6. PRESUPUESTO

Flujo de caja

Ingresos		30000
Sueldos Y salarios		20000
Depreciación		2000
Gasto financiero		0
Impuestos 25%		650
Utilidad neta		1950
Valores de salvamento		0
Valor de recuperación terreno		0
Valor de recuperación capital trabajo		0
(+) Depreciación		200
(-) Abono de capital		0
FNE	-5300	2150

7. RECURSOS

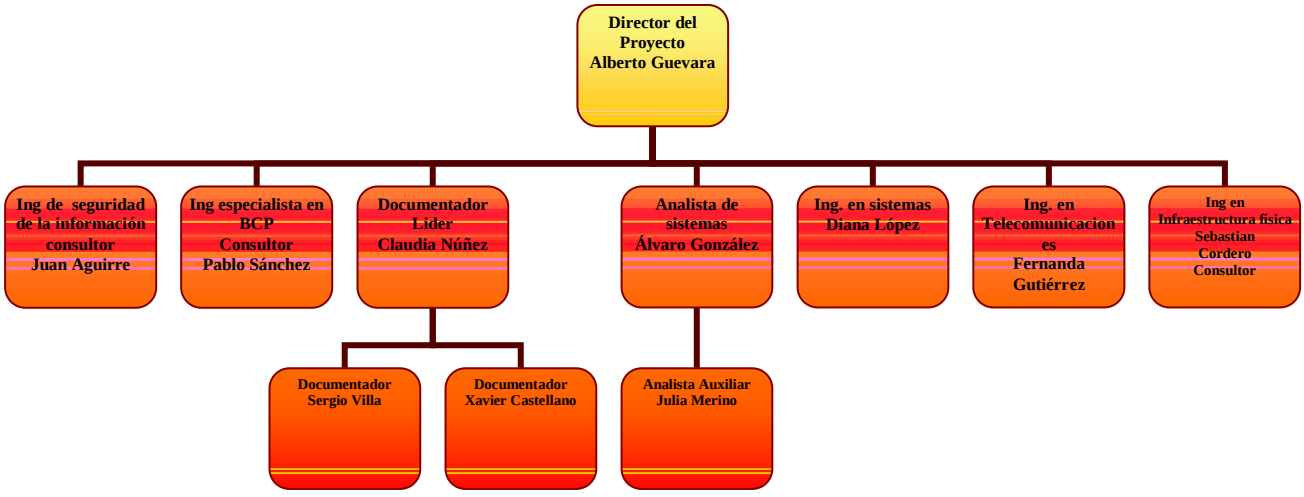
Id	Nombre	Iniciales	Tipo
1	Fernanda Gutierrez	F	Trabajo
2	Sebastian Cordero	S	Trabajo
3	Diana Lopez	D	Trabajo
4	Claudia Nuñez	C	Trabajo
5	Sergio Villa	S	Trabajo
6	Juan Aguirre	J	Trabajo
7	Xavier Castellano	X	Trabajo
8	Alberto Guevara	A	Trabajo
9	Pablo Sanchez	P	Trabajo
10	Julia Merino	J	Trabajo
11	Alvaro Gonzalez	A	Trabajo

8. RIESGOS

- El constante avance tecnológico que puede dejar obsoleto el análisis
- Las políticas de confidencialidad de las empresas financieras, las mismas que al no darnos apertura a conocer su infraestructura haría que nuestro análisis no sea real
- La probabilidad de un porcentaje mínimo de mejora

9. ORGANIZACIÓN DEL PROYECTO

1.4 ORGANIGRAMA DEL PROYECTO



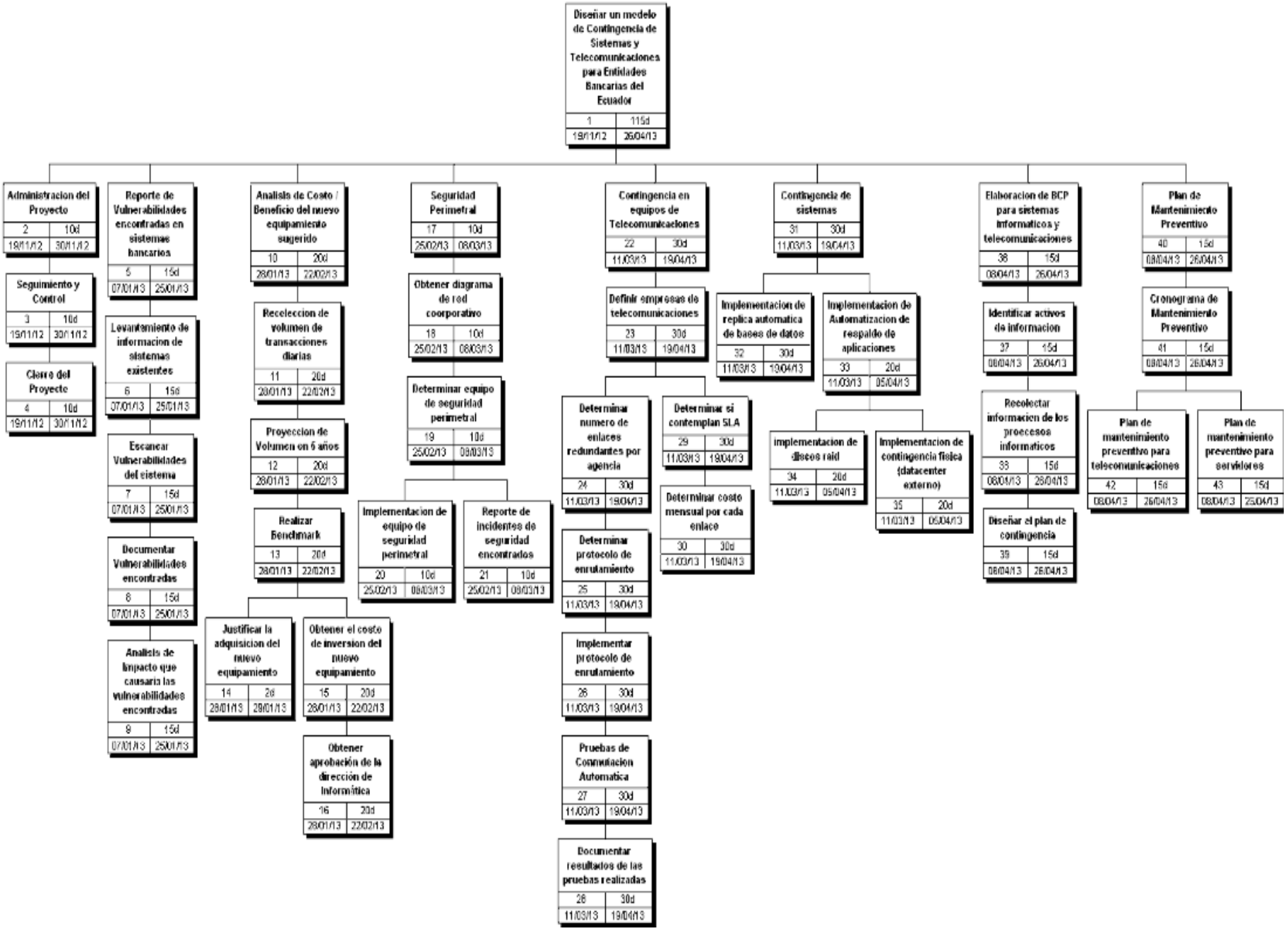
1.5 RESPONSABILIDADES

Nombre de tarea	Nombre del recurso	Trabajo
Cierre del Proyecto	Alberto Guevara	80h
Análisis de Impacto que causaria las vulnerabilidades encontradas	Alberto Guevara	120h
Justificar la adquisicion del nuevo equipamiento	Alberto Guevara	16h
Obtener aprobación de la direccion de Informatica	Alberto Guevara	160h
Implementación de equipo de seguridad perimetral	Juan Aguirre	80h
Reporte de incidentes de seguridad encontrados	Juan Aguirre	80h
Reporte de incidentes de seguridad encontrados	Xavier Castellano	80h
Documentar resultados de las pruebas realizadas	Sebastian Cordero	240h
Documentar resultados de las pruebas realizadas	Sergio Villa	240h
Documentar resultados de las pruebas realizadas	Xavier Castellano	240h
Documentar resultados de las pruebas realizadas	Julia Merino	240h
Documentar resultados de las pruebas realizadas	Alvaro Gonzalez	240h
Determinar costo mensual por cada enlace	Alberto Guevara	240h
Implementacion de replica automatica de bases de datos	Diana Lopez	240h
implementacion de discos raid	Sebastian Cordero	160h
Implementacion de contingencia fisica (datacenter externo)	Sebastian Cordero	160h
Diseñar el plan de contingencia	Pablo Sanchez	120h
Plan de mantenimiento preventivo para telecomunicaciones	Fernanda Gutierrez	120h
Plan de mantenimiento preventivo para servidores	Sebastian Cordero	120h
Plan de mantenimiento preventivo para servidores	Diana Lopez	120h

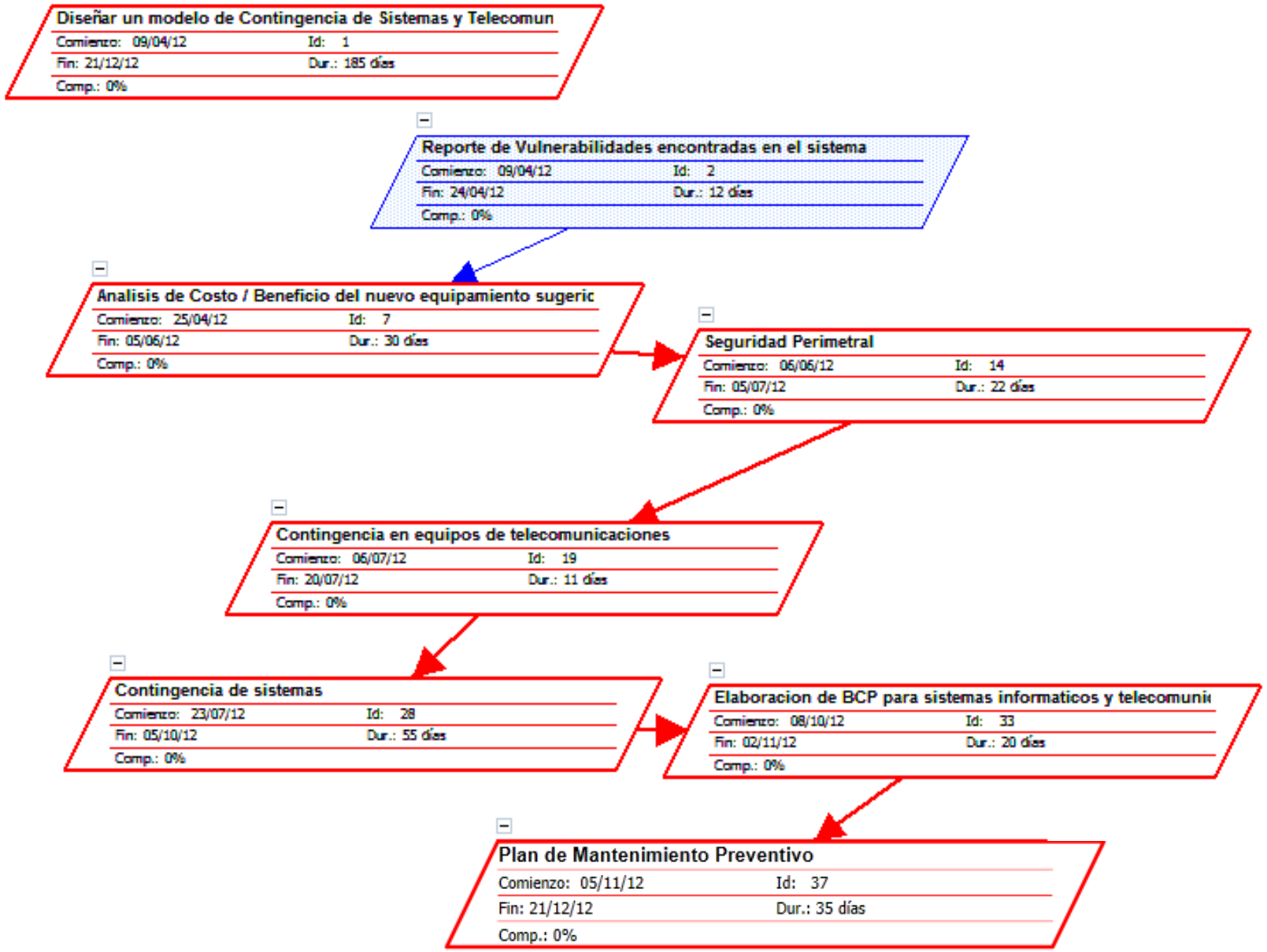
10. APROBACIÓN DEL ACTA

Cargo	*Nombre*	*Firma*	*Fecha*
Representante del Sponsor			
Program Manager			
Project Manager			

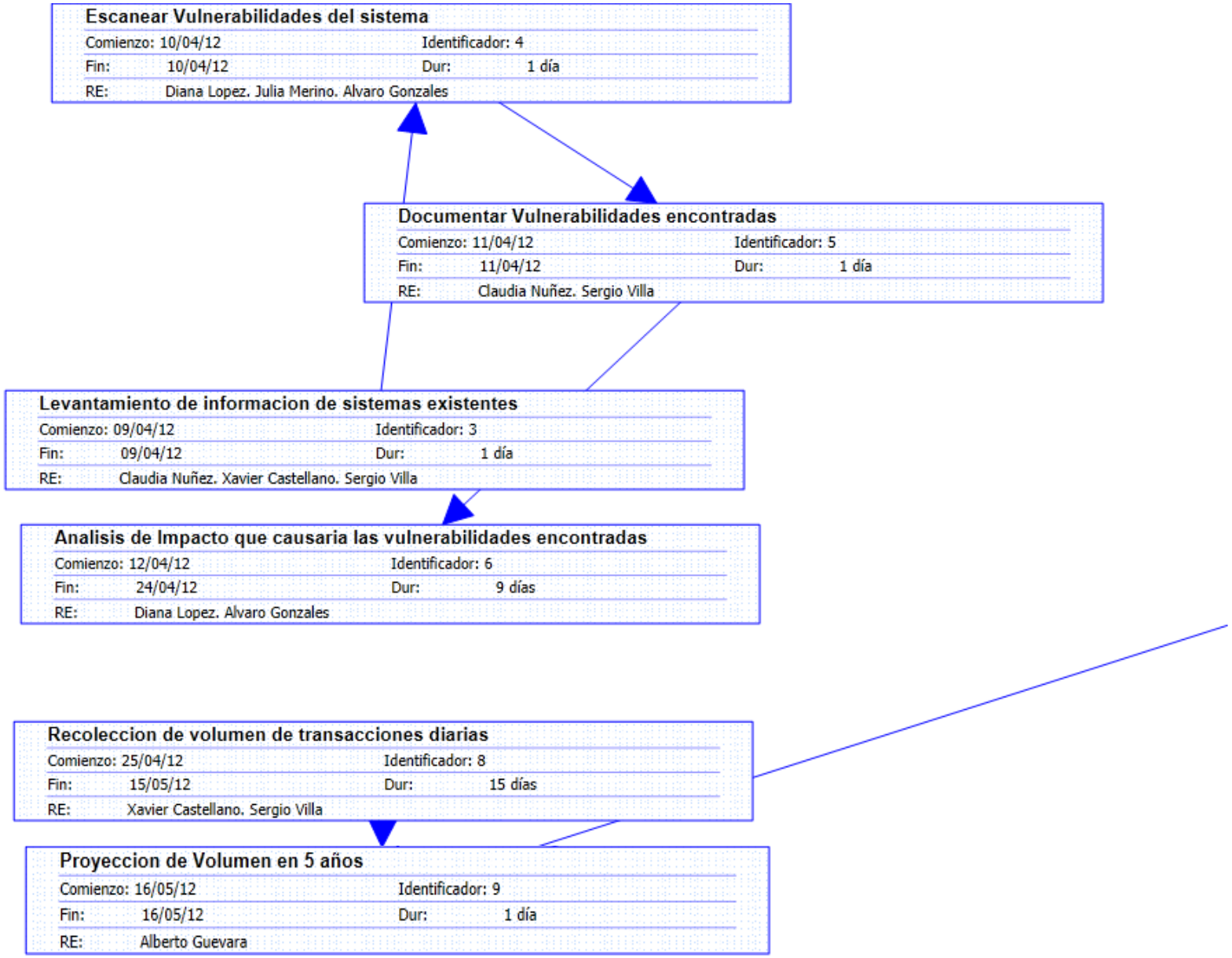
ANEXO 2 ESTRUCTURA DE DESGLOSE DE TAREAS



ANEXO 4 DIAGRAMA DE RED

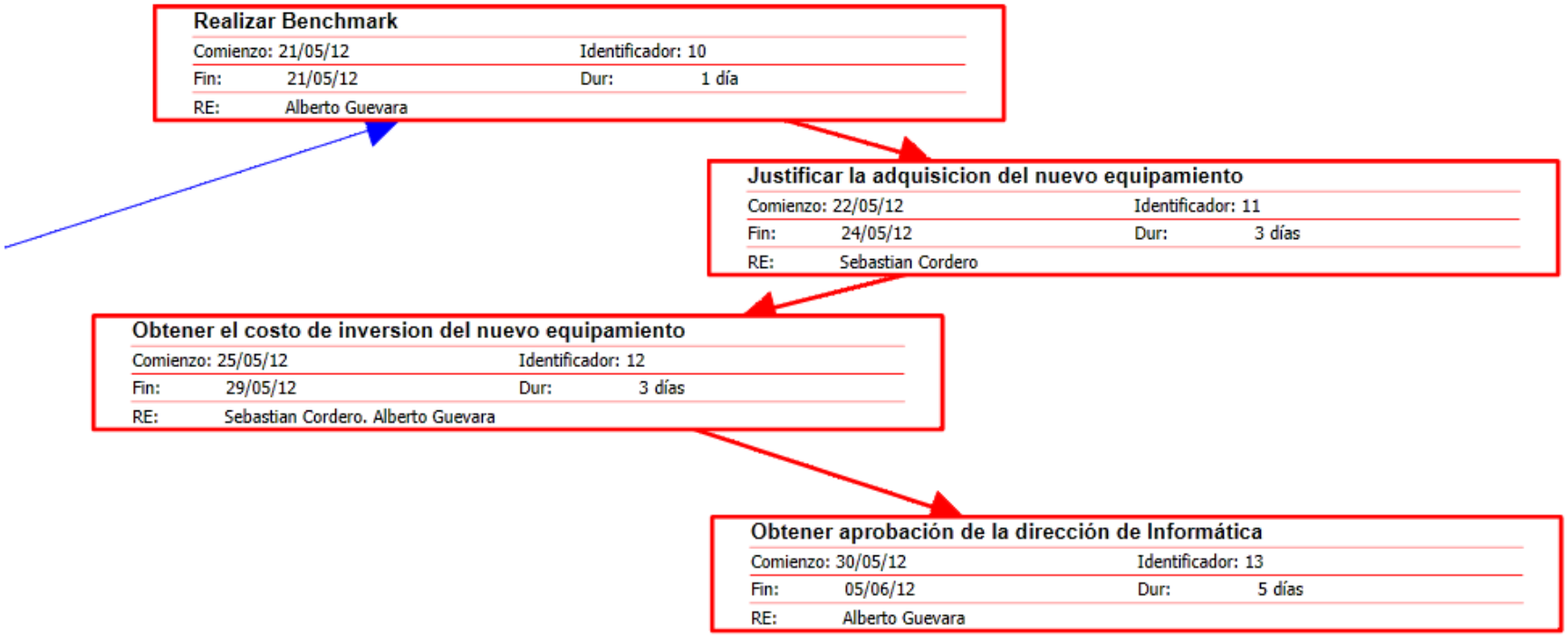


ANEXO 4 DIAGRAMA DE RED

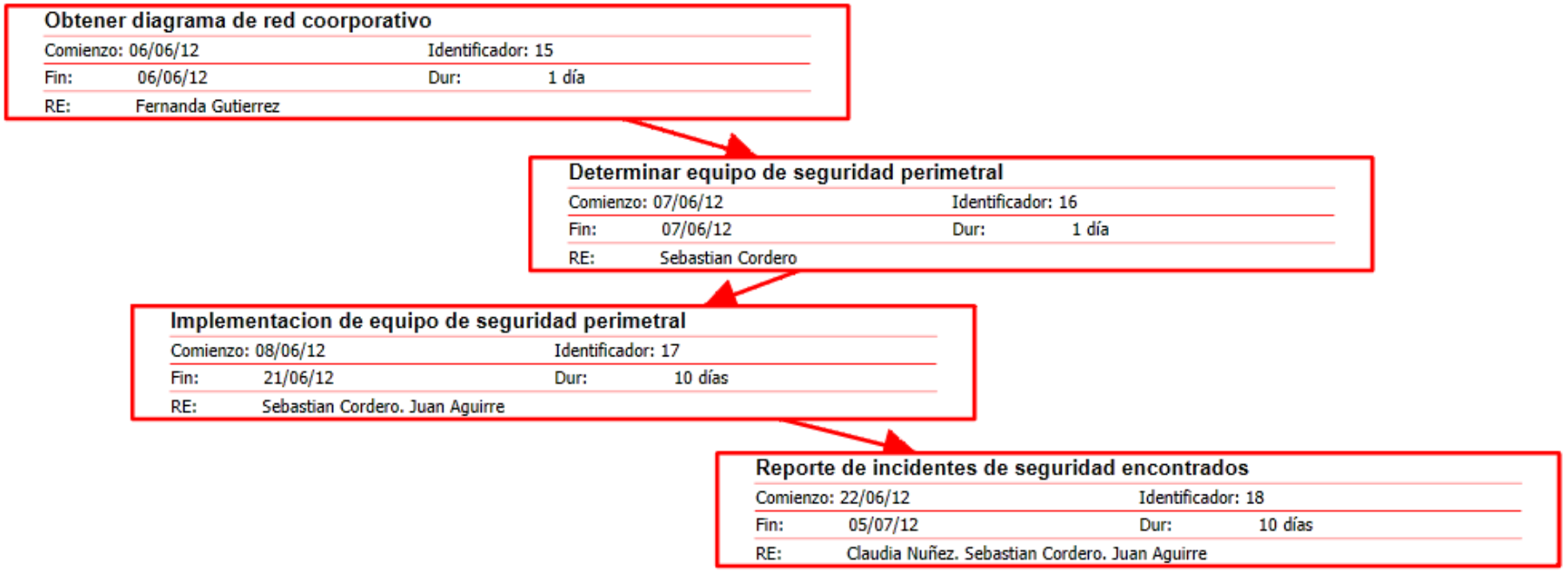


ANEXO 4 DIAGRAMA DE RED

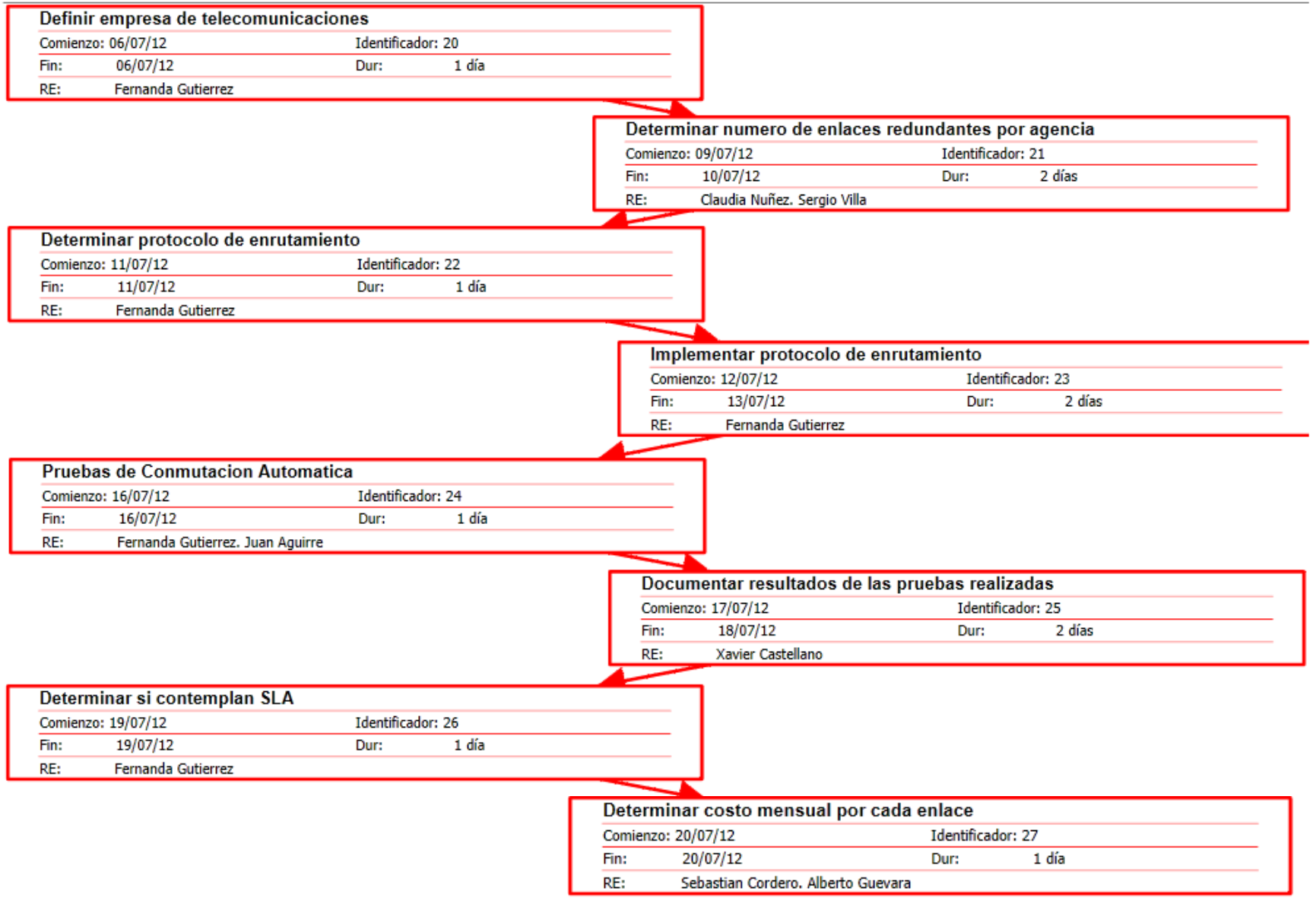
ANEXO 4 DIAGRAMA DE RED



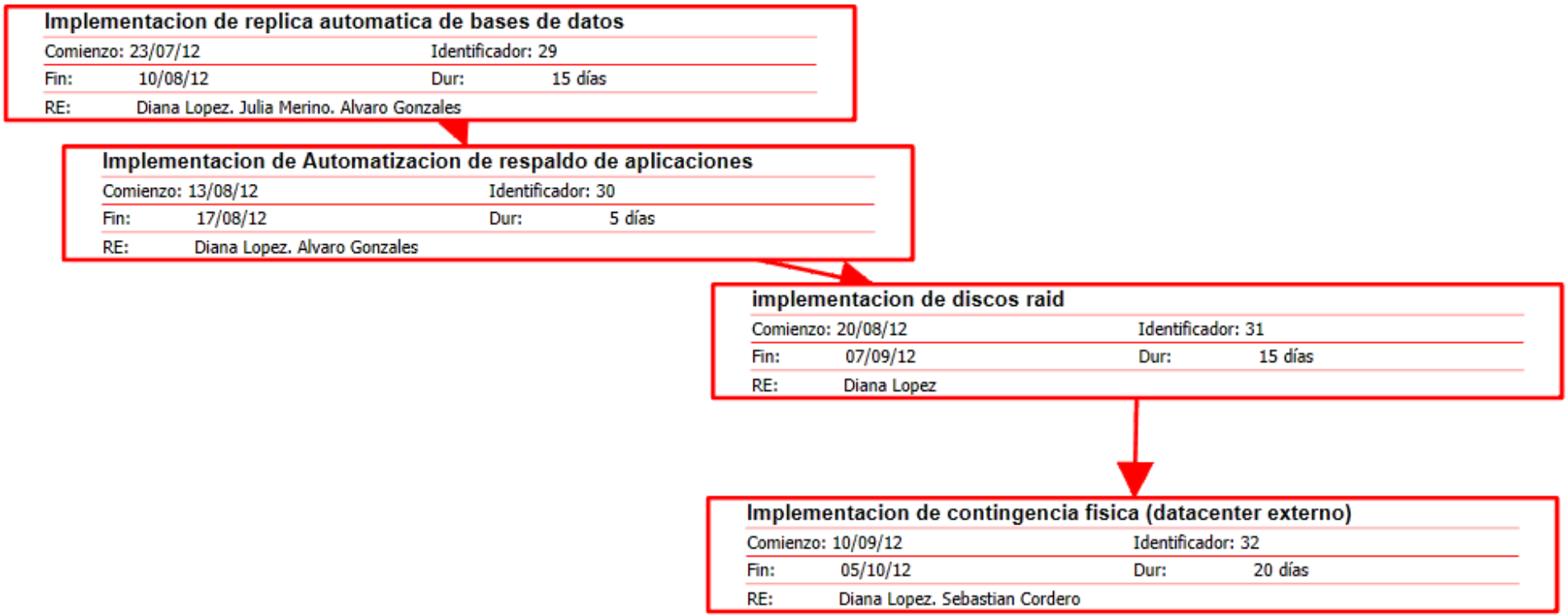
ANEXO 4 DIAGRAMA DE RED



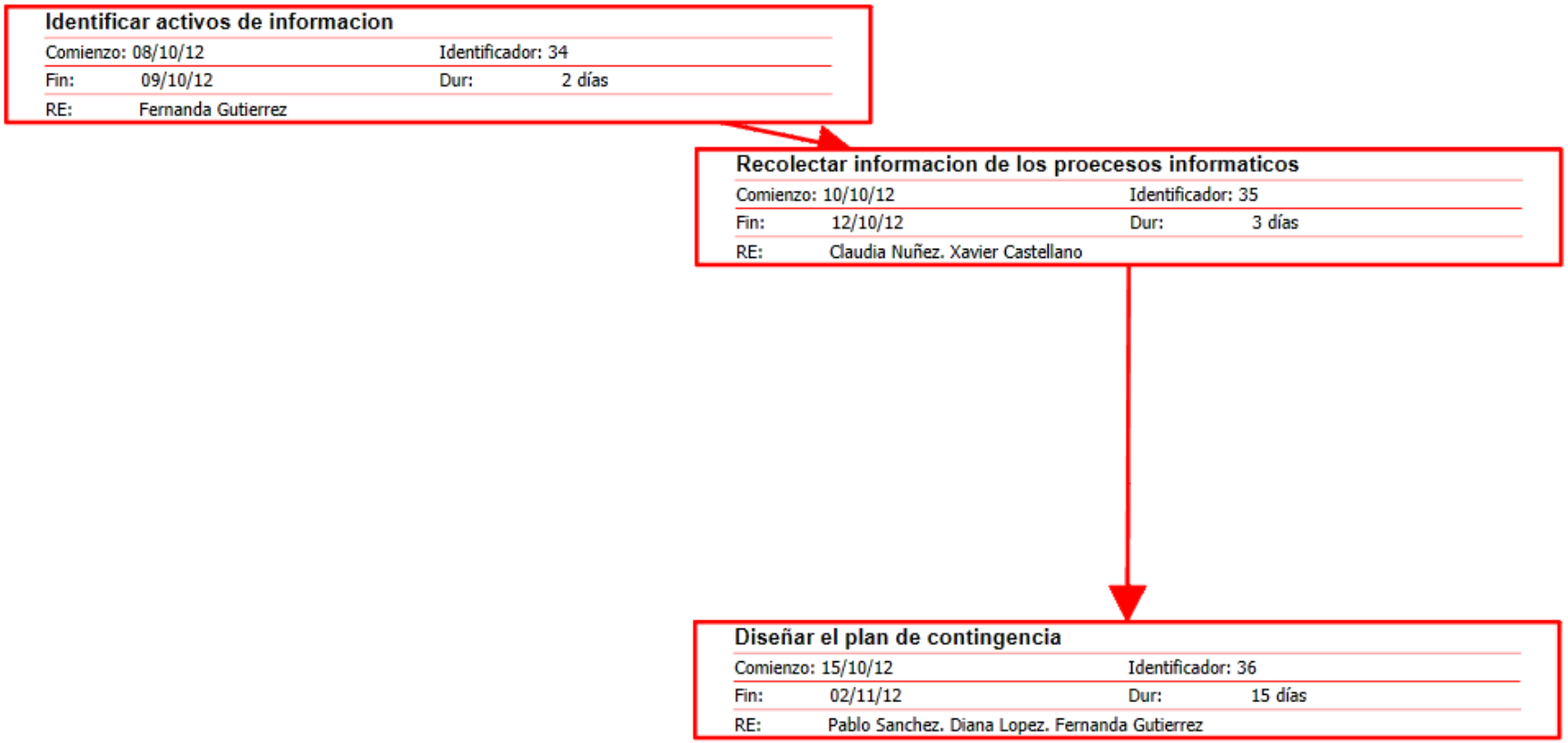
ANEXO 4 DIAGRAMA DE RED



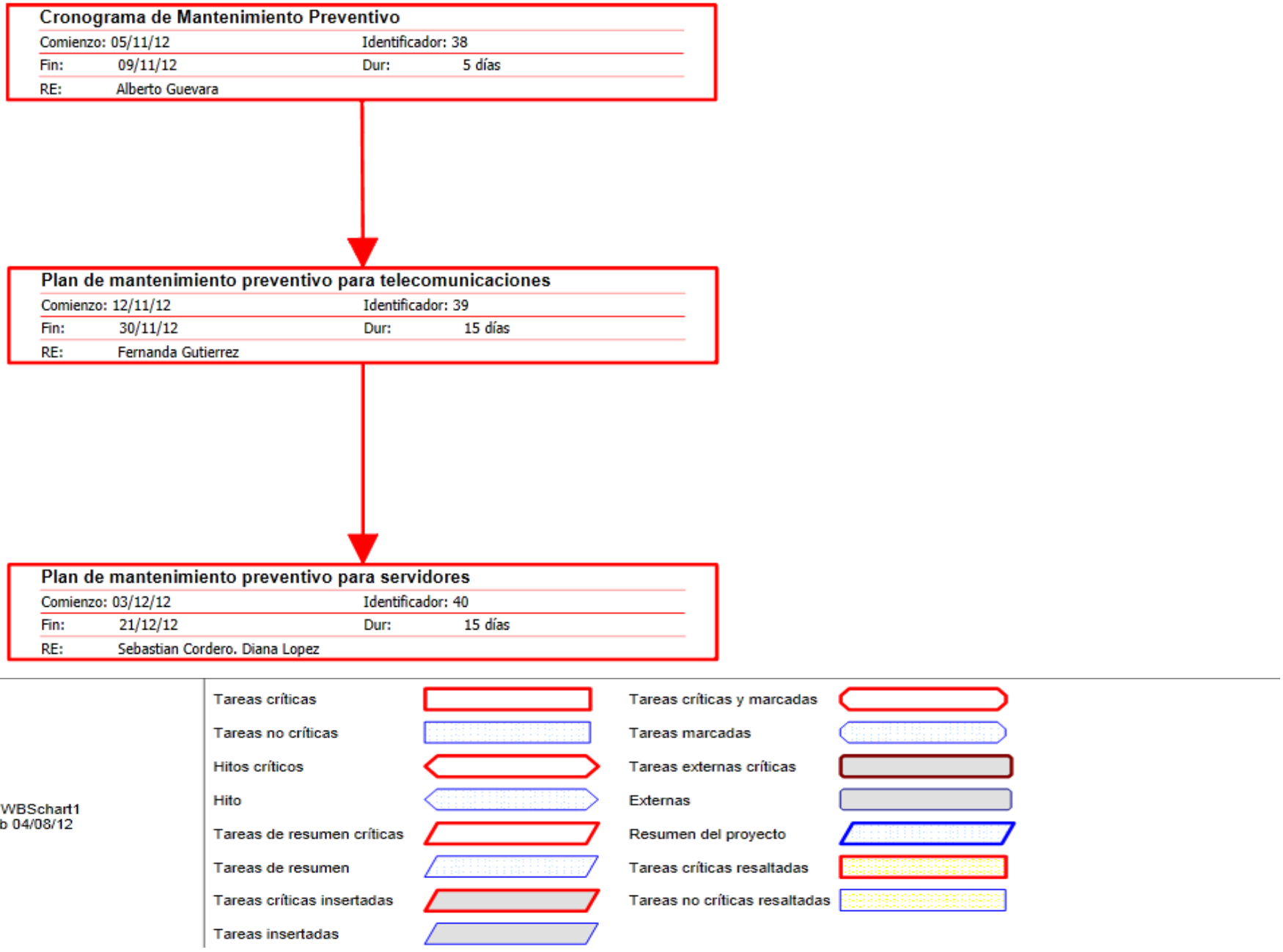
ANEXO 4 DIAGRAMA DE RED



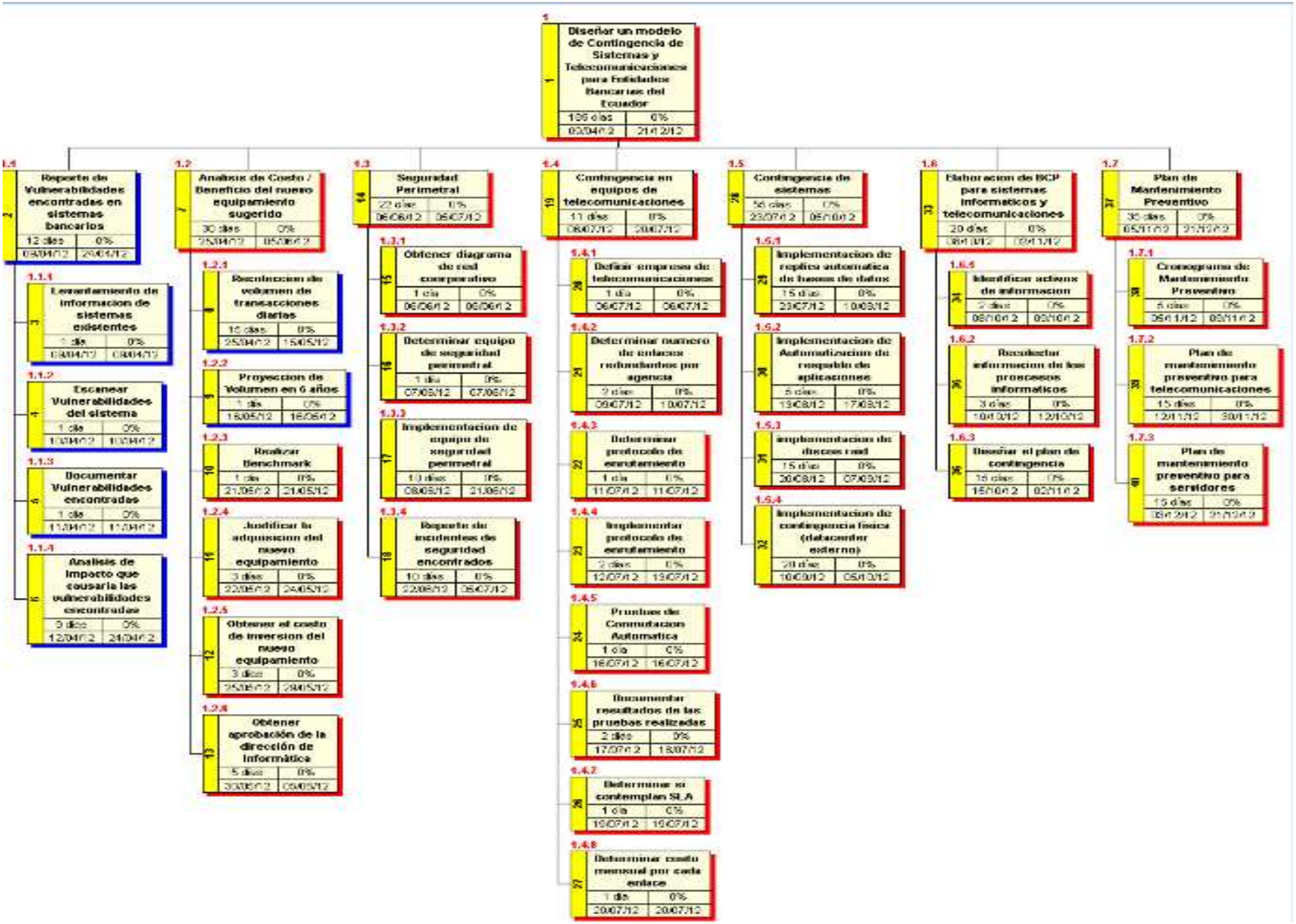
ANEXO 4 DIAGRAMA DE RED



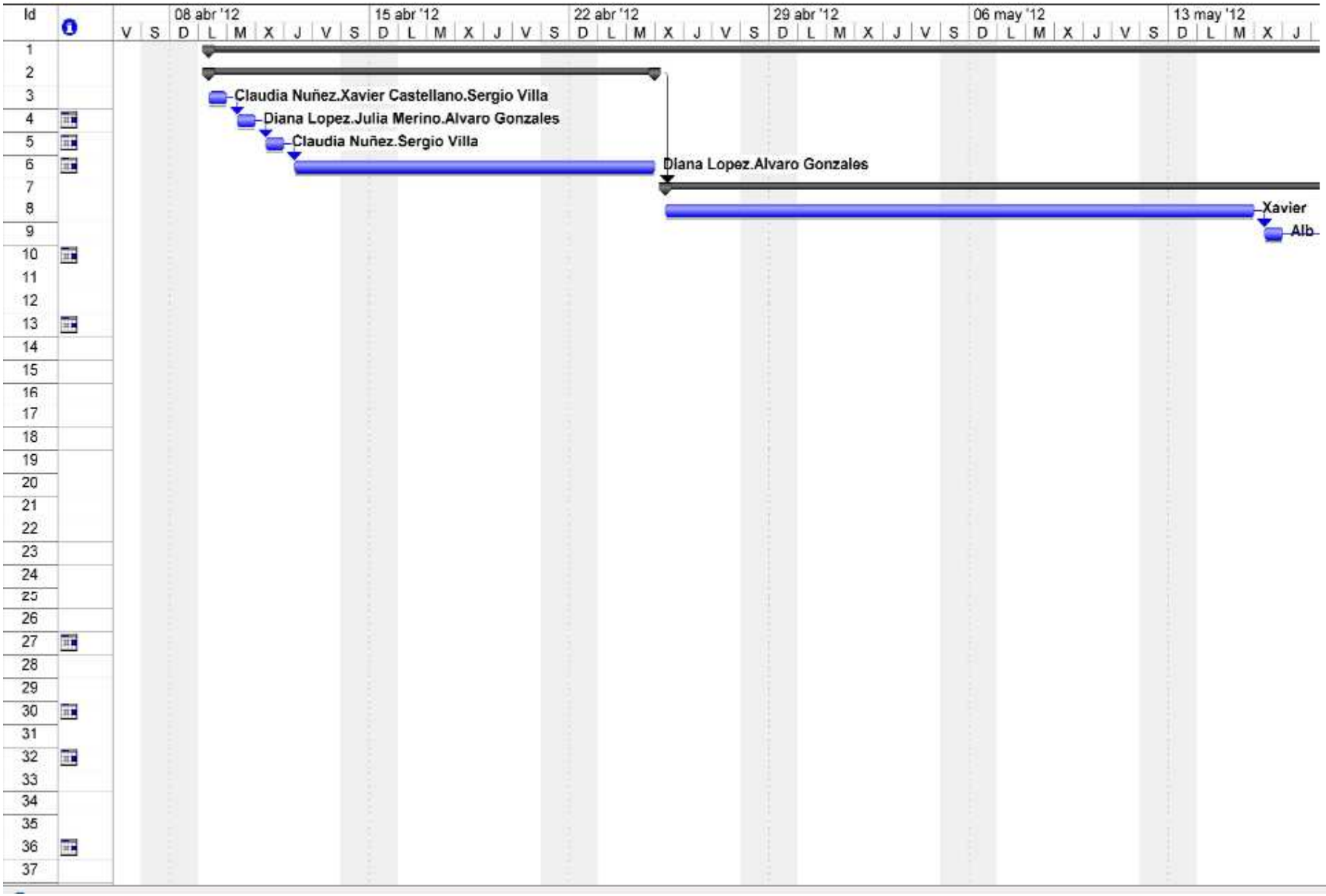
ANEXO 4 DIAGRAMA DE RED



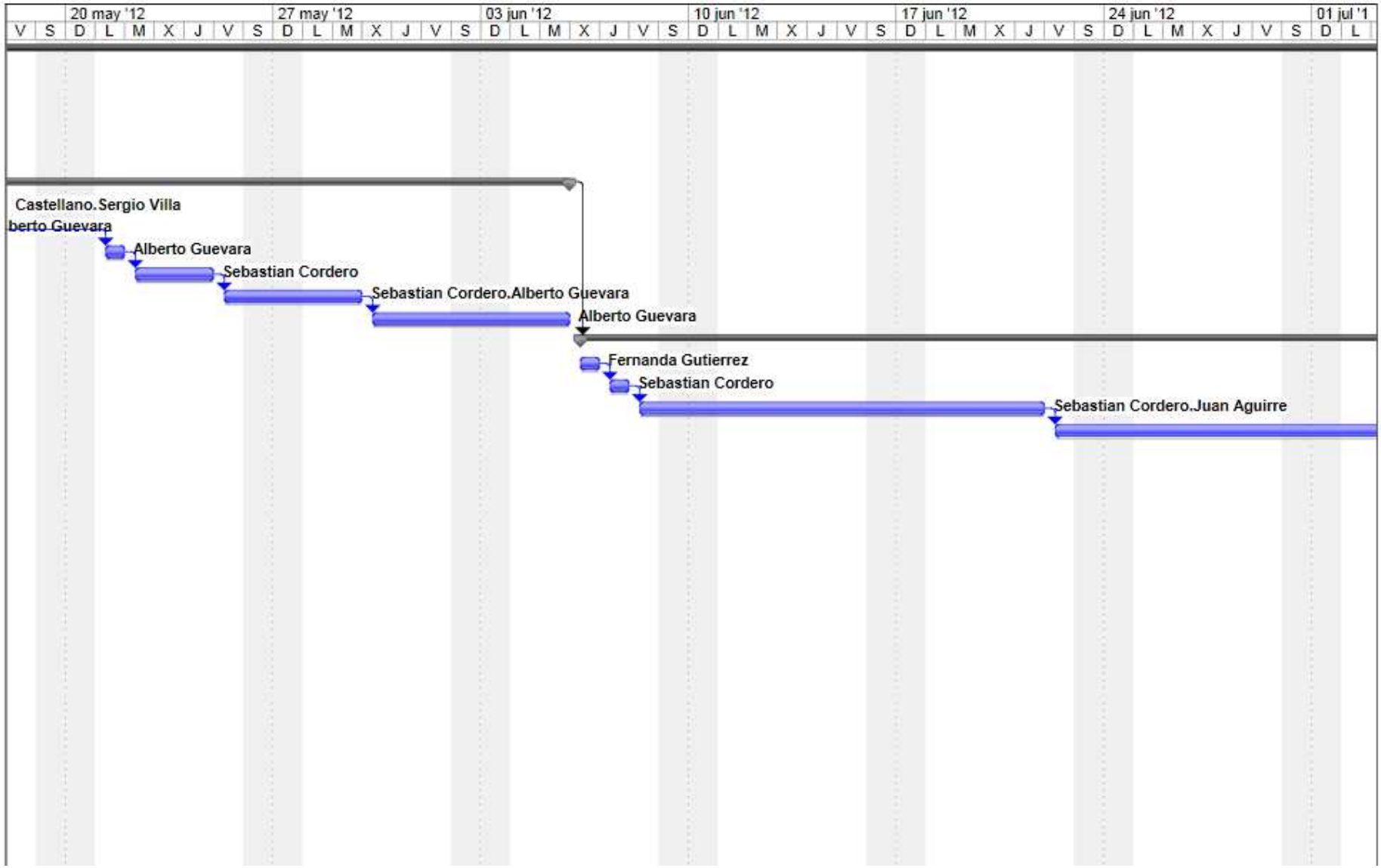
ANEXO 4 DIAGRAMA DE RED


1
Diseñar un modelo de Contingencia de Sistemas y Telecomunicaciones para Entidades Bancarias del Ecuador
106 días | 0%
02/04/12 | 21/12/12
1.1
Reporte de Vulnerabilidades encontradas en sistemas bancarios
12 días | 0%
02/04/12 | 24/04/12
1.1.1
3
Levantamiento de información de sistemas existentes
1 día | 0%
02/04/12 | 02/04/12
1.1.2
4
Escanear Vulnerabilidades del sistema
1 día | 0%
10/04/12 | 10/04/12
1.1.3
6
Documentar Vulnerabilidades encontradas
1 día | 0%
11/04/12 | 11/04/12
1.1.4
5
Analisis de Impacto que causaria las vulnerabilidades encontradas
3 días | 0%
12/04/12 | 24/04/12
1.2
7
Analisis de Costo / Beneficio del nuevo equipamiento sugerido
30 días | 0%
25/04/12 | 05/06/12
1.2.1
8
Recoleccion de volumen de transacciones diarias
15 días | 0%
25/04/12 | 15/05/12
1.2.2
9
Proyeccion de Volumen en 6 años
1 día | 0%
16/05/12 | 16/05/12
1.2.3
10
Realizar Benchmark
1 día | 0%
21/05/12 | 21/05/12
1.2.4
11
Justificar la adquisicion del nuevo equipamiento
3 días | 0%
22/05/12 | 24/05/12
1.2.5
12
Obtener el costo de inversion del nuevo equipamiento
3 días | 0%
25/05/12 | 29/05/12
1.2.6
13
Obtener aprobación de la dirección de Informática
5 días | 0%
30/05/12 | 05/06/12
1.3
14
Seguridad Perimetral
22 días | 0%
06/06/12 | 05/07/12
1.3.1
15
Obtener diagrama de red corporativo
1 día | 0%
06/06/12 | 06/06/12
1.3.2
16
Determinar equipo de seguridad perimetral
1 día | 0%
07/06/12 | 07/06/12
1.3.3
17
Implementacion de equipo de seguridad perimetral
10 días | 0%
08/06/12 | 21/06/12
1.3.4
18
Reporte de incidentes de seguridad encontrados
10 días | 0%
22/06/12 | 05/07/12
1.4
19
Contingencia en equipos de telecomunicaciones
11 días | 0%
06/07/12 | 20/07/12
1.4.1
20
Definir empresa de telecomunicaciones
1 día | 0%
06/07/12 | 06/07/12
1.4.2
21
Determinar numero de enlaces redundantes por agencia
2 días | 0%
09/07/12 | 10/07/12
1.4.3
22
Determinar protocolo de enrutamiento
1 día | 0%
11/07/12 | 11/07/12
1.4.4
23
Implementar protocolo de enrutamiento
2 días | 0%
12/07/12 | 13/07/12
1.4.5
24
Pruebas de Conmutacion Automatica
1 día | 0%
16/07/12 | 16/07/12
1.4.6
25
Documentar resultados de las pruebas realizadas
2 días | 0%
17/07/12 | 18/07/12
1.4.7
26
Determinar si contemplan SLA
1 día | 0%
19/07/12 | 19/07/12
1.4.8
27
Determinar costo mensual por cada enlace
1 día | 0%
20/07/12 | 20/07/12
1.5
28
Contingencia de sistemas
52 días | 0%
23/07/12 | 05/10/12
1.5.1
29
Implementacion de replica automatica de bases de datos
15 días | 0%
23/07/12 | 10/08/12
1.5.2
30
Implementacion de Automatizacion de respaldo de aplicaciones
5 días | 0%
13/08/12 | 17/08/12
1.5.3
31
implementacion de discos raid
15 días | 0%
20/08/12 | 07/09/12
1.5.4
32
Implementacion de contingencia física (datacenter externo)
20 días | 0%
10/09/12 | 05/10/12
1.6
33
Elaboracion de BCP para sistemas informaticos y telecomunicaciones
20 días | 0%
08/10/12 | 02/11/12
1.6.4
34
Identificar activos de información
2 días | 0%
08/10/12 | 09/10/12
1.6.2
35
Recolectar información de los procesos informaticos
3 días | 0%
10/10/12 | 12/10/12
1.6.3
36
Diseñar el plan de contingencia
15 días | 0%
15/10/12 | 02/11/12
1.7
37
Plan de Mantenimiento Preventivo
35 días | 0%
05/11/12 | 21/12/12
1.7.1
38
Cronograma de Mantenimiento Preventivo
5 días | 0%
05/11/12 | 09/11/12
1.7.2
39
Plan de mantenimiento preventivo para telecomunicaciones
15 días | 0%
12/11/12 | 30/11/12
1.7.3
40
Plan de mantenimiento preventivo para servidores
15 días | 0%
03/12/12 | 21/12/12

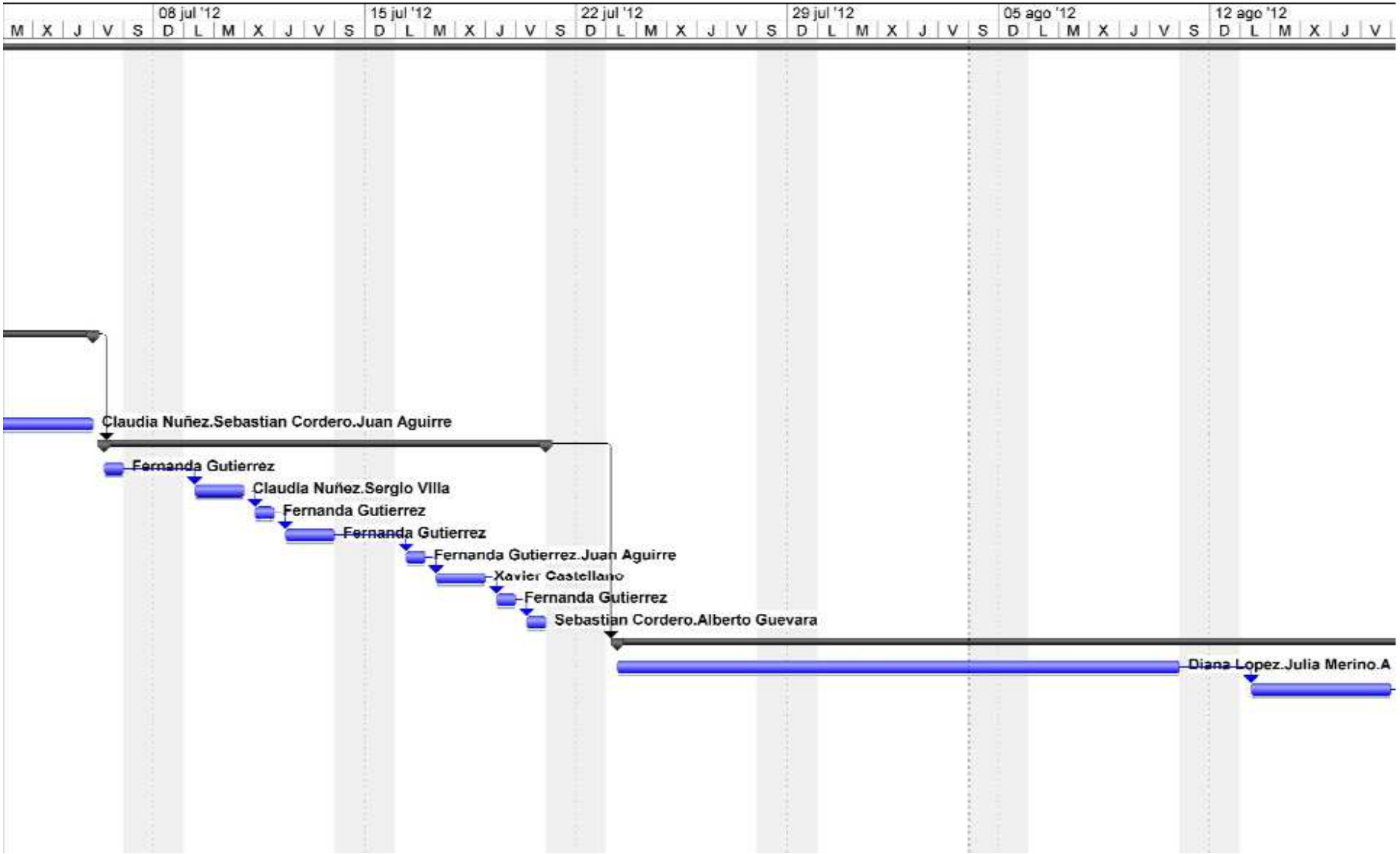
ANEXO 6 DIAGRAMA DE GANTT



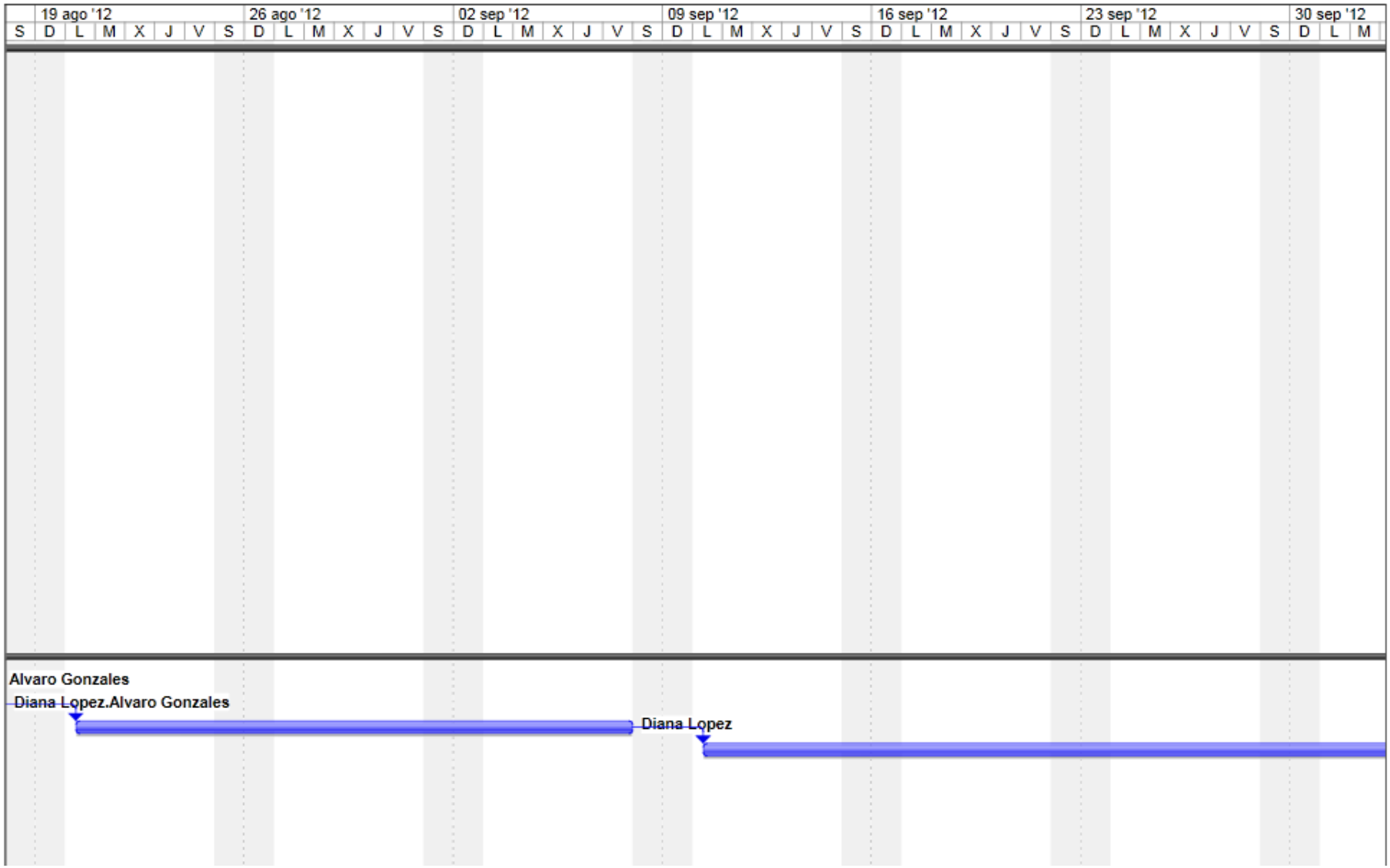
ANEXO 6 DIAGRAMA DE GANTT



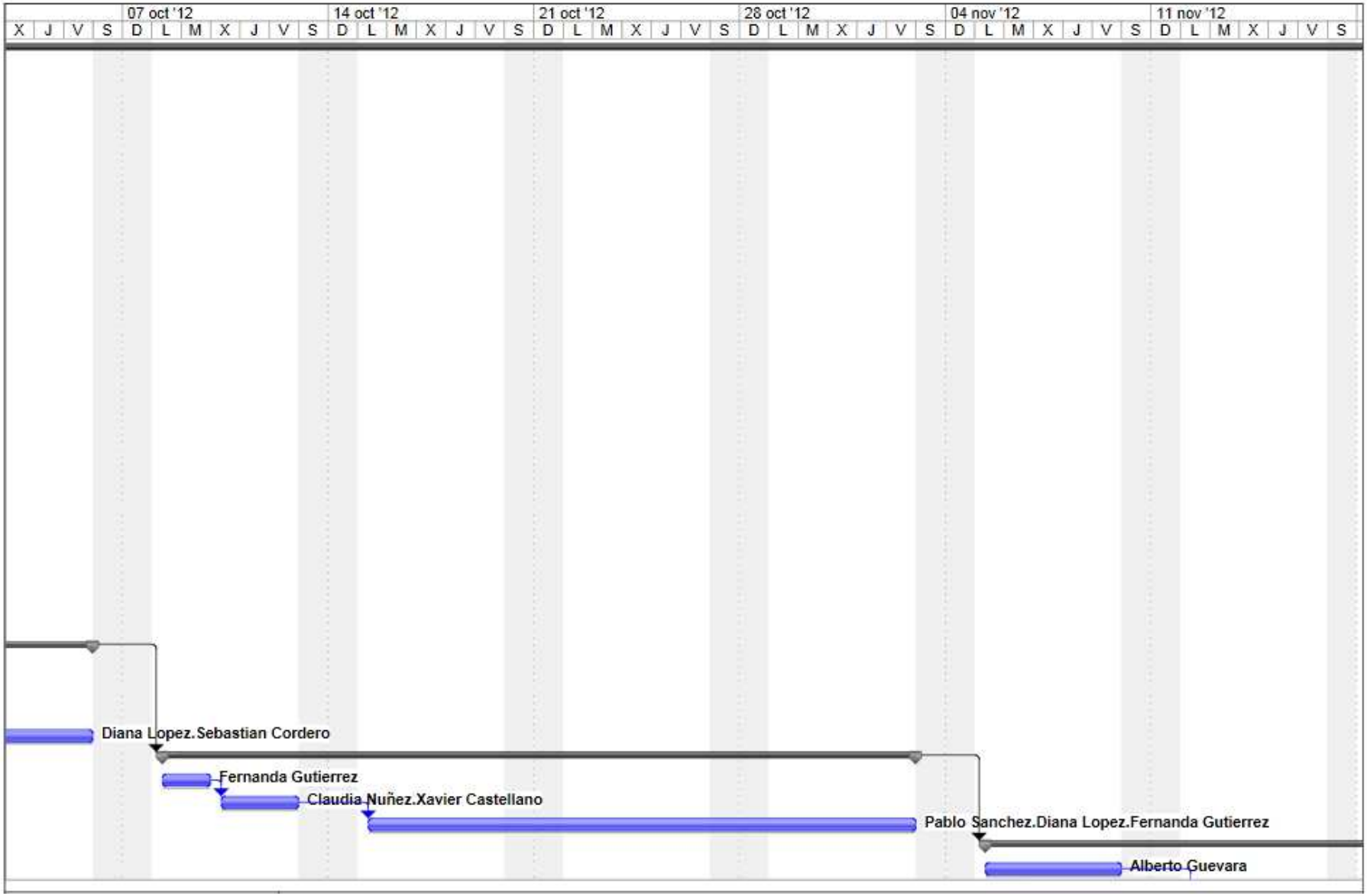
ANEXO 6 DIAGRAMA DE GANTT



ANEXO 6 DIAGRAMA DE GANTT



ANEXO 6 DIAGRAMA DE GANTT



ANEXO 6 DIAGRAMA DE GANTT