ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

ELABORACIÓN DEL PLAN DE DISPONIBILIDAD DE TI PARA LA EMPRESA RELIANCE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

JAVIER EDUARDO BAÑOS ANDI
javier.banos@hotmail.com

PAMELA AMPARITO CARRERA SUBÍA
pamelacarrera17@gmail.com

DIRECTOR: MSC. ING. RAÚL CÓRDOVA
raul.cordova@epn.edu.ec

Quito, Septiembre 2010

DECLARACIÓN

Nosotros, Baños Andi Javier Eduardo y Carrera Subía Pamela Amparito, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluye en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____	_____
Sr. Javier Baños	Srta. Pamela Carrera
CI: 1719869347	CI: 1718368325
Nro. Único: 200420042	Nro. Único: 200410214

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Baños Andi Javier Eduardo y Carrera Subía Pamela Amparito, bajo mi supervisión.

_____

Msc. Ing. Raúl Córdova
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios por llenarme de bendiciones y de mucha salud día a día.

A mi madre que con su fortaleza y dedicación, ha sido fuente de motivación para alcanzar varios de mis objetivos.

A mi amigo Jacobo por su apoyo incondicional durante los inicios de estudio de esta carrera universitaria.

A todos mis amigos y compañeros de la EPN, con los cuales vivimos momentos felices y supimos sobresalir en cada uno de los proyectos de la carrera, esto incluye por todas las amanecidas y locuras vividas con ellos.

Al Ing. Raúl Córdova, por dedicar su tiempo e impartir sus conocimientos y consejos en la realización de este proyecto.

A la empresa RELIANCE S.A y a todo su personal, por toda la colaboración prestada en la realización de este proyecto.

Javier

DEDICATORIA

A mi madre, quien me dio la vida y ha sido mi guía y fuente de inspiración. Por todo el sacrificio que ella ha realizado para que yo alcanzase mis metas, y que desde el inicio de mis estudios este objetivo no sólo ha sido mío, sino también el de ella. Por su fortaleza y dedicación para que nunca me faltase nada y tuviera oportunidades de superarme, y porque sin su bendición nada de esto sería posible.

A todos aquellos amigos y amigas que estuvieron y están conmigo en los momentos más importantes de mi vida.

Javier

AGRADECIMIENTO

Agradezco en primer lugar a mi familia por su apoyo y guía durante mi vida.

A Juan gracias por todo tu tiempo, apoyo y en especial por no dejarme desistir de continuar adelante a pesar de todo.

A mis amigos por su acolite durante todos estos años, gracias por su tiempo y paciencia.

A los profesores por impartir sus conocimientos y sabios consejos para ejercer con éxito la profesión, especialmente al Ing. Raúl Córdova por su paciencia y guía.

Un especial agradecimiento para el personal de RELIANCE S.A por su confianza y colaboración para la realización de este trabajo.

Pamela

DEDICATORIA

A las personas que amo quienes han estado a mi lado apoyándome en cada una de mis decisiones y me han animado a continuar adelante a pesar de las adversidades.

Gracias por su apoyo incondicional y sus consejos.

Pamela

CONTENIDO

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA 1

1.1. DESCRIPCIÓN DE LA EMPRESA 1
1.1.1. LA EMPRESA RELIANCE 1
1.1.2. DATOS GENERALES 1
1.1.3. MISIÓN, VISIÓN, OBJETIVOS ESTRATÉGICOS Y VALORES DE RELIANCE 2
1.1.3.1. MISIÓN 2
1.1.3.2. VISIÓN 2
1.1.3.3. OBJETIVOS ESTRATÉGICOS 2
1.1.3.4. VALORES 3
1.1.4. LA PRESENCIA DE RELIANCE EN ECUADOR 4
1.1.5. ESTRUCTURA ORGANIZACIONAL 4
1.2. PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TI DE LA EMPRESA 8
1.2.1. EL DEPARTAMENTO DE TI DENTRO DE LA EMPRESA 8
1.2.2. ÁREAS ADMINISTRATIVAS DEL DEPARTAMENTO DE TI 9
1.2.2.1. PERSONAL DEL ÁREA DE SISTEMAS 9
1.2.2.2. HARDWARE 9
1.2.2.3. OTROS DISPOSITIVOS 10
1.2.2.4. SERVICIOS DE INTERNET Y BASE DE DATOS 10
1.2.3. DESCRIPCIÓN DE LOS SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TI 11
1.2.4. MAPEO DE SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TI A LAS AÉREAS DEL NEGOCIO 14
1.2.5. LISTADO DE LOS PROCESOS DEL DEPARTAMENTO DE TI 20
1.3. NECESIDAD DE LA DISPONIBILIDAD DE TI PARA LA EMPRESA RELIANCE 22
1.4. BENEFICIOS, COSTOS Y PROBLEMAS DE LA INDISPONIBILIDAD 22
1.4.1. BENEFICIOS DE LA DISPONIBILIDAD 22
1.4.2. COSTOS DE LA DISPONIBILIDAD 23
1.4.3. PROBLEMAS DE LA INDISPONIBILIDAD 23

CAPÍTULO 2. PROCESO PARA LA ELABORACIÓN DEL PLAN DE DISPONIBILIDAD 25

2.1. DETERMINACIÓN DE REQUISITOS DE DISPONIBILIDAD 25
2.1.1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) 26
2.1.1.1. OBJETIVOS, ALCANCE DEL BIA 26
2.1.1.2. IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DEL NEGOCIO 26
2.1.1.3. EVALUACIÓN DE IMPACTO FINANCIERO Y OPERACIONAL 27
2.1.1.3.1. EVALUACIÓN DEL IMPACTO FINANCIERO 27
2.1.1.3.2. EVALUACIÓN DEL IMPACTO OPERACIONAL 28
2.1.1.4. IDENTIFICACIÓN DE PROCESOS CRÍTICOS DEL NEGOCIO 28
2.1.1.5. IDENTIFICACIÓN DE SISTEMAS Y APLICACIONES CRÍTICAS DE TI POR PROCESO DEL NEGOCIO 29
2.1.1.6. IDENTIFICACIÓN DE TIEMPOS MÁXIMOS DE CAÍDA (MTD) 29
2.1.1.7. IDENTIFICACIÓN DEL TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) Y DEL TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT) 30
2.1.1.7.1. TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) 30
2.1.1.7.2. TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT) 30
2.1.1.7.3. EVALUACIÓN DE RTO Y WRT 31
2.1.1.8. IDENTIFICACIÓN DEL OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO) 31

2.1.1.9. ANÁLISIS DEL DAÑO A CONSECUENCIA DE LA INTERRUPCIÓN DE UN SERVICIO DE TI 31
2.1.2. FUNCIONES VITALES DEL NEGOCIO 32
2.1.3. REQUISITOS DE DISPONIBILIDAD 32
2.1.3.1. ALCANCE 33
2.1.3.2. RESUMEN DE DISPONIBILIDAD DE SERVICIO TI 33
2.1.3.3. REQUERIMIENTOS DE DISPONIBILIDAD 33
2.2. DISEÑO DE LA DISPONIBILIDAD 33
2.2.1. DISEÑO DE LA INFRAESTRUCTURA TI 34
2.2.1.1. ELEMENTOS DE LA RED 35
2.2.1.2. ADMINISTRACIÓN DE TI 36
2.2.1.3. ALMACENAMIENTO 36
2.2.1.4. IMPRESIÓN Y DIGITALIZACIÓN 36
2.2.1.5. CONSIDERACIONES PARA EL HARDWARE Y SOFTWARE 37
2.2.1.5.1. CONSIDERACIONES DE HARDWARE 37
2.2.1.5.2. CONSIDERACIONES DE SOFTWARE 37
2.2.1.6. CONSIDERACIONES PARA EL ENTORNO DE LA INFRAESTRUCTURA DE TI 37
2.2.2. ANÁLISIS DE PUNTOS INDIVIDUALES DE FALLO DE COMPONENTES (SPOF) 38
2.2.2.1. ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE (CFIA) 38
2.2.2.2. ANÁLISIS POR ARBOLES DE FALLOS (FTA) 39
2.2.3. GESTIÓN Y ANÁLISIS DE RIESGO 40
2.2.3.1. MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS (CRAMM) 42
2.2.3.1.1. VALORACIÓN DE ACTIVOS 42
2.2.3.1.2. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS 42
2.2.3.1.3. IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES 43
2.2.3.1.4. EVALUACIÓN DE NIVELES DE RIESGOS 43
2.2.3.1.5. OPCIONES DE CONTROL DE RIESGOS 43
2.3. DISEÑO DE LA RECUPERACIÓN 44
2.3.1. ELEMENTOS PRINCIPALES DEL DISEÑO DE LA RECUPERACIÓN 44
2.3.2. GESTIÓN DE SISTEMAS 45
2.3.3. CAPTURA DE DATOS PARA EL DIAGNOSTICO 45
2.3.4. NECESIDADES DE RECUPERACIÓN Y BACKUP 45
2.3.5. MÉTRICAS DE RECUPERACIÓN 46
2.4. CONSIDERACIONES DE SEGURIDAD 46
2.4.1. SEGURIDAD DE LA INFORMACIÓN 47
2.4.2. SEGURIDAD FÍSICA Y AMBIENTAL 48
2.4.3. SEGURIDAD DE LOS EQUIPOS 48
2.4.4. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES 48
2.4.5. RESPALDO O BACK-UP 48
2.4.6. SEGURIDAD DE LA RED 48
2.4.7. MONITOREO 49
2.4.8. ROLES Y RESPONSABILIDADES 49
2.5. MANTENIMIENTO DEL PLAN 50
2.5.1. MONITORIZACIÓN Y ANÁLISIS DE LAS TENDENCIAS DE GESTIÓN DE LA DISPONIBILIDAD .. 51
2.5.2. DETERMINAR LOS REQUISITOS DE DISPONIBILIDAD (Modificados) 51
2.5.3. EL COSTO DE MEJORAR LA DISPONIBILIDAD 51
2.5.4. MÉTODOS Y TÉCNICAS 51

CAPÍTULO 3. ELABORACIÓN DEL PLAN DE DISPONIBILIDAD DE TI PARA LA EMPRESA RELIANCE 53

3.1. ACTIVIDADES VITALES DEL NEGOCIO 55
3.1.1. ACTIVIDADES DEL NEGOCIO RELACIONADAS CON TI 55
3.1.2. ACTIVIDADES CLAVES DEL NEGOCIO RELACIONADAS CON TI 59

3.2. ELEMENTOS DE CONFIGURACIÓN (CI) 62
3.2.1. ELEMENTOS DE CONFIGURACIÓN DE HARDWARE 62
3.2.1.1. ORDENADORES 63
3.2.1.2. IMPRESORAS 64
3.2.1.3. SWITCH 65
3.2.1.4. MODEM 65
3.2.1.5. INTERFACES DE RED 66
3.2.1.6. UNIDADES DE ALMACENAMIENTO 66
3.2.1.7. ALIMENTADOR DE ENERGÍA ALTERNA (UPS) 68
3.2.2. ELEMENTOS DE CONFIGURACIÓN DE SOFTWARE 68
3.2.2.1. HERRAMIENTAS 68
3.2.2.2. SISTEMAS DE GESTIÓN DE BRÓKERES DE SEGUROS 72
3.2.2.3. SISTEMAS OPERATIVOS 73
3.3. DETERMINACIÓN DE REQUISITOS DE DISPONIBILIDAD 73
3.3.1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) 73
3.3.1.1. OBJETIVOS Y ALCANCE 73
3.3.1.1.1. OBJETIVOS 73
3.3.1.1.2. ALCANCE 74
3.3.1.2. IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DEL NEGOCIO 74
3.3.1.3. EVALUACIÓN DE IMPACTO FINANCIERO Y OPERACIONAL 76
3.3.1.3.1. EVALUACIÓN DEL IMPACTO FINANCIERO 76
3.3.1.3.2. EVALUACIÓN DEL IMPACTO OPERACIONAL 77
3.3.1.4. IDENTIFICACIÓN DE PROCESOS CRÍTICOS DEL NEGOCIO 83
3.3.1.5. IDENTIFICACIÓN DE SISTEMAS Y APLICACIONES CRÍTICAS DE TI POR PROCESO DEL NEGOCIO 89
3.3.1.6. IDENTIFICACIÓN DE TIEMPOS MÁXIMOS DE CAÍDA (MTD) 90
3.3.1.7. IDENTIFICACIÓN DEL TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) Y DEL TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT) 94
3.3.1.7.1. TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) 94
3.3.1.7.2. TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT) 94
3.3.1.7.3. EVALUACIÓN DE RTO Y WRT 95
3.3.1.8. IDENTIFICACIÓN DEL OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO) 97
3.3.1.9. ANÁLISIS DEL DAÑO A CONSECUENCIA DE LA INTERRUPCIÓN DE UN SERVICIO DE TI 99
3.3.2. FUNCIONES VITALES DEL NEGOCIO 101
3.3.3. REQUISITOS DE DISPONIBILIDAD 106
3.3.3.1. ALCANCE 107
3.3.3.2. RESUMEN DE DISPONIBILIDAD DE SERVICIO TI 107
3.3.3.3. REQUERIMIENTOS DE DISPONIBILIDAD 108
3.4. DISEÑO DE LA DISPONIBILIDAD 125
3.4.1. DISEÑO DE LA INFRAESTRUCTURA TI 125
3.4.1.1. ELEMENTOS DE LA RED 125
3.4.1.2. ADMINISTRACIÓN DE TI 126
3.4.1.3. ALMACENAMIENTO 126
3.4.1.4. IMPRESIÓN Y DIGITALIZACIÓN 127
3.4.1.5. CONSIDERACIONES PARA EL HARDWARE Y SOFTWARE 127
3.4.1.5.1. CONSIDERACIONES DE HARDWARE 127
3.4.1.5.2. CONSIDERACIONES DE SOFTWARE 128
3.4.1.6. CONSIDERACIONES PARA EL ENTORNO DE LA INFRAESTRUCTURA DE TI 128
3.4.1.7. ANÁLISIS DE PUNTOS INDIVIDUALES DE FALLO DE COMPONENTES (SPOF) 132
3.4.1.7.1. ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE (CFIA) 132
3.4.1.7.2. ANÁLISIS POR ÁRBOLES DE FALLOS (FTA) 138
3.4.1.8. GESTIÓN Y ANÁLISIS DE RIESGO 141
3.4.1.8.1. MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS (CRAMM) 141
3.4.1.8.1.1. VALORACIÓN DE ACTIVOS 141

3.4.1.8.1.2. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS 142
3.4.1.8.1.3. IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES 143
3.4.1.8.1.4. EVALUACIÓN DE NIVELES DE RIESGOS 145
3.4.1.8.1.5. OPCIONES DE CONTROL DE RIESGOS 147
3.5. DISEÑO DE LA RECUPERACIÓN 150
3.5.1. ELEMENTOS PRINCIPALES DEL DISEÑO DE LA RECUPERACIÓN 151
3.5.2. GESTIÓN DE SISTEMAS 151
3.5.3. CAPTURA DE DATOS PARA EL DIAGNÓSTICO 151
3.5.4. NECESIDADES DE RECUPERACIÓN Y "BACKUP" 153
3.5.5. MÉTRICAS DE RECUPERACIÓN 154
3.5.6. MÉTRICAS DE TIEMPO 154
3.5.7. MÉTRICAS DE COSTOS 155
3.5.8. MÉTRICAS DE EFECTIVIDAD DEL PLAN DE RECUPERACIÓN 156
3.5.9. RESTAURACIÓN Y COMPROBACIÓN DEL SERVICIO 157
3.6. CONSIDERACIONES DE SEGURIDAD 157
3.6.1. SEGURIDAD DE LA INFORMACIÓN 157
3.6.2. SEGURIDAD FÍSICA Y AMBIENTAL 158
3.6.3. SEGURIDAD DE LOS EQUIPOS 159
3.6.4. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES 159
3.6.5. RESPALDO O BACK-UP 160
3.6.6. SEGURIDAD DE LA RED 161
3.6.7. MONITOREO 161
3.7. MANTENIMIENTO DEL PLAN 162
3.7.1. MONITORIZACIÓN Y ANÁLISIS DE LAS TENDENCIAS DE GESTIÓN DE LA DISPONIBILIDAD 162
3.7.2. DETERMINAR LOS REQUISITOS DE DISPONIBILIDAD (Modificados) 163
3.7.3. EL COSTO DE MEJORAR LA DISPONIBILIDAD 164
3.7.4. MÉTODOS Y TÉCNICAS 164

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES 165

4.1. CONCLUSIONES 165
4.2. RECOMENDACIONES 166

BIBLIOGRAFÍA 169

ANEXOS 172

ANEXOS DIGITALES 172

ÍNDICE DE TABLAS

TABLA 1.1: EQUIPOS INFORMÁTICOS ADMINISTRADOS POR EL DEPARTAMENTO DE TI 10
TABLA 1.2: OTROS DISPOSITIVOS ADMINISTRADOS POR EL DEPARTAMENTO DE TI..... 10
TABLA 1.3: SERVICIOS QUE DA SOPORTE EL DEPARTAMENTO DE TI..... 14
TABLA 1.4: MAPEO DE SERVICIOS 19
TABLA 1.5: LISTADO DE PROCESOS DEL DEPARTAMENTO DE TI 21
TABLA 3.1: ACTIVIDADES DEL NEGOCIO RELACIONADAS CON TI..... 59
TABLA 3.2: ACTIVIDADES CLAVES DEL NEGOCIO RELACIONADAS CON TI 61
TABLA 3.3: ORDENADORES ADMINISTRADOS POR EL DEPARTAMENTO DE TI..... 64
TABLA 3.4: IMPRESORAS MATRICIALES Y DE TINTA EN RED ADMINISTRADA POR EL DEPARTAMENTO DE TI 64
TABLA 3.5: IMPRESORA MULTIFUNCIÓN EN RED ADMINISTRADA POR EL DEPARTAMENTO DE TI 65
TABLA 3.6: SWITCH ADMINISTRADO POR EL DEPARTAMENTO DE TI 65
TABLA 3.7: MODEM ADMINISTRADO POR EL DEPARTAMENTO DE TI 65
TABLA 3.8: INTERFACES DE RED ADMINISTRADAS POR EL DEPARTAMENTO DE TI..... 66
TABLA 3.9: UNIDADES DE ALMACENAMIENTO ADMINISTRADAS POR EL DEPARTAMENTO DE TI..... 67
TABLA 3.10: ALIMENTADOR DE ENERGÍA ALTERNA ADMINISTRADO POR EL DEPARTAMENTO DE TI..... 68
TABLA 3.11: APLICACIONES DE SOFTWARE ADMINISTRADAS POR EL DEPARTAMENTO DE TI 69
TABLA 3.12: FRECUENCIA DE USO DE LAS APLICACIONES DE SOFTWARE ADMINISTRADAS POR EL DEPARTAMENTO DE TI 69
TABLA 3.13: FRECUENCIA DE USO POR PC DE LAS HERRAMIENTAS DE SOFTWARE ADMINISTRADAS POR EL DEPARTAMENTO DE TI 72
TABLA 3.14: SISTEMA DE GESTIÓN DE BROKERS DE SEGUROS ADMINISTRADO POR EL DEPARTAMENTO DE TI..... 72
TABLA 3.15: SISTEMAS OPERATIVOS ADMINISTRADOS POR EL DEPARTAMENTO DE TI..... 73
TABLA 3.16: FUNCIONES Y PROCESOS DE RELIANCE..... 76
TABLA 3.17: ANÁLISIS DE IMPACTO FINANCIERO..... 78
TABLA 3.18: EVALUACIÓN DEL IMPACTO OPERACIONAL 83
TABLA 3.19: PROCESOS CRÍTICOS DEL NEGOCIO..... 88
TABLA 3.20: SISTEMAS Y APLICACIONES CRÍTICAS DE TI POR PROCESO DEL NEGOCIO..... 90
TABLA 3.21: ESCALA DE EQUIVALENCIA DE MTD 91
TABLA 3.22: DEFINICIÓN DE MTD..... 93
TABLA 3.23: TOTAL DE VALORES DE MTD'S DEL NEGOCIO 93
TABLA 3.24: TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) DE LAS ACTIVIDADES DE TI 95
TABLA 3.25: RTO Y WRT POR PROCESOS DEL NEGOCIO..... 96
TABLA 3.26: OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO) POR PROCESOS DEL NEGOCIO 98
TABLA 3.27: CONSECUENCIAS DE LA INTERRUPCIÓN DE UN SERVICIO DE TI..... 101
TABLA 3.28: FUNCIONES VITALES DEL NEGOCIO 106
TABLA 3.29: COLORACIÓN DE LA TABLA DE FUNCIONES VITALES DEL NEGOCIO 106
TABLA 3.30: RESUMEN DE DISPONIBILIDAD DE SERVICIOS TI DE RELIANCE 108
TABLA 3.31: SALA PRINCIPAL DE EQUIPOS INFORMÁTICOS 129
TABLA 3.32: SALA DE EQUIPOS DE REDES Y SERVIDORES..... 130
TABLA 3.33: ENTORNO DE OFICINA 131
TABLA 3.34: MATRIZ DE CONFIGURACIÓN DEL ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE DE RELIANCE..... 136
TABLA 3.35: CFIA QUE REFLEJA LAS RELACIONES ENTRE COMPONENTES, ÁREAS DEL NEGOCIO Y USUARIOS FINALES AFECTADOS..... 138
TABLA 3.36: ACTIVOS TI 142
TABLA 3.37: TIPOS DE AMENAZAS 143

TABLA 3.38: VULNERABILIDADES 145
TABLA 3.39: EVALUACIÓN DE NIVELES DE RIESGOS 146
TABLA 3.40: OPCIONES DE CONTROL DE RIESGOS 150
TABLA 3.41: MÉTRICAS DE COMPONENTES DE TI 152
TABLA 3.42: NECESIDADES DE RECUPERACIÓN Y BACKUP 154

ÍNDICE DE FIGURAS

FIGURA 1.1: ORGANIGRAMA DE RELIANCE 5
FIGURA 1.2: TOPOLOGÍA DE RED DE RELIANCE 12
FIGURA 2.1: ANÁLISIS Y GESTIÓN DE RIESGOS 41
FIGURA 3.1: PROCESOS DE LA GESTIÓN DE LA DISPONIBILIDAD 55
FIGURA 3.2: CONFIGURACIÓN DEL ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE EN RELIANCE 133
FIGURA 3.3: ANÁLISIS DE ÁRBOL DE FALLOS DEL SISTEMA SIBROK 139
FIGURA 3.4: ANÁLISIS DE ÁRBOL DE FALLOS DEL SERVIDOR DE CORREO ELECTRÓNICO 140

RESUMEN

El presente proyecto de titulación propone el Desarrollo del Plan de Disponibilidad de TI para un bróker de seguros, con el objetivo de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, dándole así continuidad de operaciones a sus principales actividades.

El Capítulo 1 consta de una descripción general de la empresa RELIANCE S.A., su principal actividad y su funcionamiento interno. También se describe su Departamento de TI, sus actividades, su estructura organizacional y un mapeo de servicios que soportan a las áreas del negocio; de manera que ayuda a tener una visión global del tipo de empresa, sus carencias y requerimientos de disponibilidad de servicios de TI.
Al final de este capítulo se describen los beneficios y costos que dispondría la organización al implementar un Plan de Disponibilidad de TI. Así también se describen los posibles problemas que se tendría a causa de la indisponibilidad de los servicios TI.

En el Capítulo 2 se describe el proceso y las actividades que se deben seguir para la elaboración del Plan de Disponibilidad de Tecnologías de la Información (TI), para pequeñas y medianas empresas, de acuerdo a la Gestión de la Disponibilidad de TI, descrito en la librería de ITIL.

En el Capítulo 3 se procede a la elaboración del Plan de Disponibilidad de TI, para la empresa RELIANCE.
La elaboración del Plan de Disponibilidad inicia con la descripción de todos los componentes necesarios para el desarrollo del proceso de la Gestión de la Disponibilidad, para lo cual primero se definen a las Actividades Vitales del Negocio, teniendo en cuenta que se realiza un mapeo de las actividades de la organización por áreas.

A continuación se determinan los Requisitos de Disponibilidad de la empresa. Estos requisitos permiten determinar las necesidades reales del negocio, con respecto a la Disponibilidad de las Tecnologías de la Información. Dentro de la determinación de requisitos de disponibilidad se realiza un Análisis de Impacto en el Negocio (BIA), así como también se determina las Funciones Vitales del Negocio.

Una vez determinados los Requisitos de Disponibilidad del negocio, se procede a desarrollar las actividades de diseño de la Disponibilidad de servicios de TI. Estas actividades permiten garantizar que se pueden satisfacer el nivel de disponibilidad requeridos por los servicios de TI. Entre las actividades de diseño constan: El Diseño de la Disponibilidad, El Diseño de la Recuperación, Consideraciones Sobre la Seguridad y Mantenimiento del Plan de Disponibilidad.

En el Capítulo 4 se presentan las conclusiones y recomendaciones generadas durante el desarrollo del presente trabajo.

PRESENTACIÓN

El Plan de Disponibilidad para TI propuesto en este proyecto de titulación, inicia realizando un análisis situacional de la empresa RELIANCE S.A., describe su actividad principal en el mercado, su misión y visión, su estructura organizacional. Se describe el funcionamiento del Departamento de TI, sus áreas funcionales, la descripción de servicios que brinda TI al negocio y un listado de procesos que gestiona el Departamento de TI; este análisis ayuda a obtener las necesidades de disponibilidad de los servicios en el negocio. Adicionalmente se describe la necesidad de la disponibilidad de ti para la empresa considerando los beneficios, costos y problemas de la indisponibilidad.

En el capítulo 2 se describe los pasos esenciales para elaborar el Plan de disponibilidad, que puede ser aplicado a cualquier organización, mientras que en el capítulo 3 se encuentra la parte práctica orienta a la empresa RELIANCE.

Previo a la elaboración del diseño del Plan de Disponibilidad de TI enfocado a la empresa RELIANCE, se identificó componentes del proceso de gestión de la disponibilidad; las actividades claves del negocio relacionadas con TI y los elementos de configuración que conforman los servicios tanto de hardware como de software.

En el diseño del Plan de Disponibilidad se inició con la identificación de requisitos de disponibilidad para los servicios de TI para ello fue necesario identificar las funciones vitales del negocio mediante un análisis de impacto en el negocio (BIA) y los elementos de configuración.

Teniendo en cuenta los requisitos identificados se realizó el diseño de la infraestructura TI el cual es la suma de todos los componentes de hardware, software y servicios profesionales necesarios para hacer funcionar las múltiples aplicaciones de tecnología de información, y que permite a la organización apoyar y automatizar los procesos del negocio.

Seguidamente se elaboró el diseño de la recuperación que se centra en los componentes del diseño necesarios para garantizar que cuando fallen los servicios, se puedan retornar las operaciones normales del negocio tan rápidamente como sea posible, además se estableció métricas de recuperación que se tomarán durante un fallo para poder mejorar los procesos de recuperación establecidos.

A continuación se plantea consideraciones de seguridad de la información, física y ambiental, de los equipos, procedimientos y responsabilidades operaciones, respaldo, seguridad de la red y actividades de monitoreo.

Finalmente las consideraciones para dar mantenimiento al plan de disponibilidad el cual debe tener fines, objetivos y resultados, y debe estudiar los aspectos relacionados con el personal, los procesos, herramientas y técnicas además de centrarse en la tecnología.

La Gestión de la Disponibilidad es responsable de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLA’s y todo ello a un costo razonable. La satisfacción del cliente y la rentabilidad de los servicios TI dependen en gran medida de su éxito.

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA

En el presente capítulo se realiza una descripción general de la empresa RELIANCE, en la cual se aplicara el desarrollo del Plan de Disponibilidad de Tecnologías de la Información (TI), mediante el uso de las buenas prácticas de la librería ITIL.

Al final de este capítulo se describen los beneficios y costos que dispondría la organización al implementar un Plan de Disponibilidad de TI. Así también se describen los posibles problemas que se tendría a causa de la indisponibilidad de los servicios TI.

1.1. DESCRIPCIÓN DE LA EMPRESA

1.1.1. LA EMPRESA RELIANCE

RELIANCE es un bróker de seguros que sirve de nexo entre los clientes y las compañías de seguros.
La empresa es una subdivisión del “Banco Promerica” antes “Banco MM Jaramillo Arteaga”. El banco es el que se encarga a su vez de entregar las solicitudes de los clientes para los servicios de aseguramiento.

1.1.2. DATOS GENERALES

Dirección: Av. Amazonas N25-23 y Colón.
Edif. España piso 7 oficina 70
Teléfonos: (593-2) 252 75 37 / 252 62 98
Fax: (593-2) 255 74 05

1.1.3. MISIÓN, VISIÓN, OBJETIVOS ESTRATÉGICOS Y VALORES DE RELIANCE

La misión, visión, objetivos estratégicos y valores de la empresa que se indican a continuación, han sido tomados del Documento “La Empresa RELIANCE S.A”[1]

1.1.3.1. MISIÓN

“Somos una empresa de intermediación asesora de productos de seguro de exitosa trayectoria orientada a la protección y seguridad de nuestros clientes; satisfaciendo sus expectativas suministrándoles soluciones integrales ya que contamos con un equipo humano comprometido en brindarle el servicio personalizado y calidad que nuestros clientes esperan”.

1.1.3.2. VISIÓN

“Ser una empresa reconocida, creando así una cultura de seguros, gracias a los conocimientos del rubro, los valores personales y el uso de tecnología de punta, la cual será un pilar fundamental al momento de llevar en forma óptima los datos de los clientes”.

1.1.3.3. OBJETIVOS ESTRATÉGICOS

- Garantizar a los asegurados la cobertura apropiada, en aseguradoras especializadas y solventes, al mejor costo y especialmente prestar un excelente servicio.
- Diversificar el recurso financiero optimizando el rendimiento de sus inversiones.
- Automatizar las operaciones de la compañía a través del desarrollo de programas y sistemas de información.

[1] Autor: Gerente General de RELIANCE

- Desarrollar y capacitar el recurso humano de la empresa a través de programas de entrenamiento en las áreas técnicas, de producción, administrativas y atención al público en general.

1.1.3.4. VALORES

RELIANCE es una empresa que se caracteriza por fomentar aquellos buenos valores que representen de forma confiable ante sus clientes.

Entre los valores que caracterizan a RELIANCE están los siguientes:

- **Calidad:** En todos los ámbitos de cada uno de los servicios que provee a sus clientes.
- **Justicia:** Hacia nuestro personal, tanto en el trato como en la asignación de actividades a realizar, dependiendo éstas de la capacidad de cada uno de ellos.
- **Innovación:** Continua de nuestras estrategias y de nuestros métodos de trabajo.
- **Coherencia:** Entre lo que nos comprometemos con nuestro cliente y lo que efectuamos como trabajo.
- **Comunicación:** Constante y efectiva, entre todos los miembros que formamos parte de la empresa, así como con nuestros proveedores y clientes.
- **Confianza:** En que realizaremos nuestras labores de la mejor manera, con la finalidad de satisfacer a cada uno de nuestros clientes.
- **Compromiso:** Con nuestro clientes, al brindarles servicios de calidad; con la sociedad, al brindar estabilidad a las familias de nuestro personal, y con el medio ambiente, al respetar y cumplir todas las normas establecidas para el cuidado de éste.
- **Imparcialidad:** Entre nuestros clientes y proveedores.
- **Visión de futuro:** comprometidos a mejorar los servicios brindados, y con ello al crecimiento y expansión de la compañía.

1.1.4. LA PRESENCIA DE RELIANCE EN ECUADOR

La matriz de RELIANCE se encuentra ubicada en la ciudad de Quito, en el mismo edificio de la matriz del Banco Promerica.
El banco cuenta con sucursales en las siguientes ciudades:

- Ibarra
- Otavalo
- Ambato
- Quito
- Riobamba
- Cuenca
- Guayaquil
- Azogues.

Las principales compañías de seguros con las que trabaja actualmente son:

- Seguros Colón
- Seguros Latina
- Equinoccial
- Humana
- Palic
- BMI

Durante los últimos tres años RELIANCE ha presentado un notable crecimiento que va de la mano con la presencia del Banco Promerica, el cual se ha constituido en un socio estratégico que le permite a RELIANCE abarcar mayor área de cobertura en el mercado laboral ecuatoriano.

1.1.5. ESTRUCTURA ORGANIZACIONAL

En la Figura 1.1 se muestra el organigrama de la empresa RELIANCE.

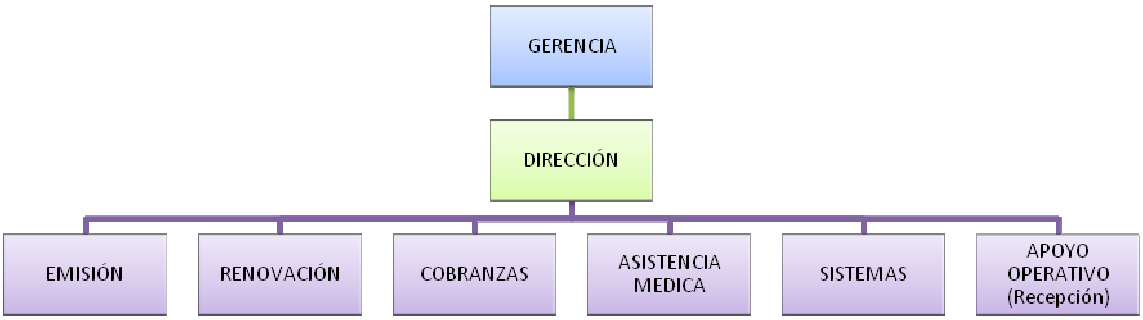

Figura 1.1: Organigrama de RELIANCE[2]

A continuación se describe a cada una de las aéreas de RELIANCE:

GERENCIA: Es el representante legal de la compañía, se encarga de las negociaciones de mejora y adquisición de los planes de seguros (pólizas) que proporcionan las diferentes aseguradoras en la región.

Además presenta informes de las actividades de la compañía y el balance a los socios de RELIANCE.

DIRECCIÓN: Se encarga de coordinar las tareas entre las distintas áreas; vigila que se estén siguiendo las normas y procedimientos establecidos para cada área y evalúa el desempeño; al dar un seguimiento continuo identifica falencias y establece mejoras a los procesos y promueve el mejoramiento continuo en la compañía.

Atiende reclamos de clientes que probablemente hablaron con los ejecutivos y están insatisfechos, además da soporte a las áreas en temas puntuales que requieren ser tratados a nivel ejecutivo.

[2] Autores: Javier Baños, Pamela Carrera, Gerente de Sistemas de RELIANCE (Santiago Granda)

Maneja el área financiera, lleva un control interno de los ingresos y egresos. Aprueba la adquisición de insumos de papelería, cafetería y tecnologías.

Adicionalmente se encarga de realizar una planificación de recursos humanos, políticas de comportamiento en la compañía, rol de pagos, asignación y contracción del personal.

EMISIÓN: Se encarga de validar el correcto ingreso de los datos en las solicitudes de seguros emitidas por el banco a sus clientes al momento de solicitar un crédito; para ser procesado el crédito en el banco, la solicitud debe ser aprobada, para lo cual el encargado del área debe confirmar los datos y reenviar la póliza a la aseguradora.

Los tipos de seguros que maneja esta área son seguros hipotecarios, desgravamen e incendio.

RENOVACIÓN: Esta área es la encargada de validar, renovar y actualizar los datos de las pólizas de seguro que los clientes poseen.
Una vez revisada y analizada la respectiva información de la póliza de seguro del cliente, se determina si el cliente posee o no crédito para la cotización de su seguro.

Si se establece la cotización del seguro con la aseguradora del cliente, se procede a la emisión de certificados para que la compañía aseguradora realice el proceso de facturación; caso contrario, se emiten y entregan notificaciones a la nueva compañía aseguradora y con ello se realiza el mismo proceso inicial de la cotización del seguro.

Para el proceso de renovación, el personal encargado de esta área obtiene la información necesaria del cliente desde el sistema SIBROK (Sistema Informático de Bróker), que permite administrar las pólizas de seguro de los clientes. En caso de no contar con la información necesaria por medio del sistema, el personal encargado realiza la gestión necesaria para contactarse con el cliente. Si al final

no se logra contactar al cliente se procede a la elaboración y entrega de avisos de vencimiento del seguro.

COBRANZAS: Esta área es la encargada realizar los cobros de las pólizas de los seguros a los clientes asegurados y con ello realizar el respectivo depósito del dinero en el banco correspondiente.

Para el cobro de los valores de las pólizas de seguro, primero se verifica que toda la información presentada por el cliente se correcta y, en caso de ser necesario, se realiza un contacto con el banco para validar toda la información.
Una vez hecho esto, se procede a realizar todo el trámite de depósito en el banco desde la emisión de recibos hasta el depósito del valor de la póliza de seguro de forma presencial en el banco.

ASISTENCIA MÉDICA: Es el área encargada de la recepción de nuevas solicitudes de seguros médicos, tramitar reclamos de cobertura de medicinas, citas médicas, operaciones, todo aquello que requiera el asegurado para mantener su salud.

En el caso de recepción de nuevas solicitudes es en esta área en donde se revisa si la documentación está completa y se la válida para luego enviarla a la aseguradora contratada.

Para reclamos se debe validar que se presenten las correspondientes justificaciones, como en el caso de haberse hecho atender en un consultorio distinto de la compañía de seguros en que se pueden presentar las facturas y una copia del resultado del reclamo. Estos son enviados a la aseguradora en donde se evalúa si es reembolsable o no. De ser así se hace llegar el cheque al afiliado o la negación con su justificación.

SISTEMAS: Esta área es la encargada del manejo, control y administración de las tecnologías de información en RELIANCE, así como de la administración y depuración de toda la información de los clientes asegurados que es enviada por

el Banco a la empresa, la misma que al final es entregada a cada una de las áreas internas para ser procesada.

Entre las tareas a cargo del departamento de **Sistemas** están las siguientes:

- Administración del sistema SIBROK
- Administración del servidor de base de datos del sistema
- Administración del servidor de correo electrónico
- Administración del programa antivirus
- Administración de la red
- Administración del Active Directory (a nivel de dominio para login)
- Soporte técnico y mantenimiento de equipos y de software
- Soporte a usuarios
- Depuración de la información
- Ingreso de pólizas de seguros
- Elaboración de reportes de producción
- Manejo de cableado y equipos electrónicos (configuración)

PERSONAL DE APOYO OPERATIVO (RECEPCIÓN): Se encarga del área de recepción y también realiza labores de contabilidad como son la emisión de cheques y manejo del libro diario, adicionalmente está a cargo del despacho de mensajería.

1.2. PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TI DE LA EMPRESA

1.2.1. EL DEPARTAMENTO DE TI DENTRO DE LA EMPRESA

El departamento de TI dentro de la empresa se encuentra ubicado en la sede de la matriz de RELIANCE, en la ciudad de Quito y es debido a su cercanía con el Banco Promerica, el cual se encuentra ubicado en el mismo edificio de RELIANCE y con ello facilita las comunicaciones entre las dos empresas, así como de su personal.

El departamento de TI es dirigido por el Gerente de Sistemas, el cual está encargado de brindar asesoría y soporte a todas las áreas administrativas de RELIANCE.

El departamento de TI es dirigido bajo políticas de control y seguridad que le permiten operar dentro de los formatos apropiados en relación a la administración de la información que le es enviada por parte del Banco Promerica.

1.2.2. ÁREAS ADMINISTRATIVAS DEL DEPARTAMENTO DE TI

1.2.2.1. PERSONAL DEL ÁREA DE SISTEMAS

Cuenta con una sola persona que se encarga de administrar el Sistema SIBROK, de realizar Backus, mantenimiento de Hardware y Software, adquisición de insumos y equipos informáticos, soporte a usuarios.

1.2.2.2. HARDWARE

En la Tabla 1.1 se presenta la una lista de equipos informáticos administrados por el departamento de TI de la empresa RELIANCE.

DEPARTAMENTO	TIPO CPU	RAM	SISTEMA OPERATIVO
Renovación de vehículos	Intel(R) Pentium(R) 4 CPU 3.20GHz	512	Windows XP Professional 5.1
Recepción	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1
Emisión y Renovación de vehículos	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1
Cobranzas	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1
Asistencia Médica	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1

DEPARTAMENTO	TIPO CPU	RAM	SISTEMA OPERATIVO
Renovación de incendio, desgravamen	Intel(R) Pentium(R) 4 CPU 2.80GHz	512	Windows XP Professional 5.1
Sistemas	Dual-Core AMD Opteron 2.80GHz	2047	Windows Server 2003 R2 5.2
Sistemas	Intel(R) Core(TM)2 CPU 6400 2.13GHz	2048	Windows XP Professional 5.1
Dirección	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1
Gerencia	Intel(R) Pentium(R) 4 CPU 2.80GHz	769	Windows XP Professional 5.1

Tabla 1.1: Equipos Informáticos Administrados por el Departamento de TI

1.2.2.3. OTROS DISPOSITIVOS

En la Tabla 1.2 se muestra el inventario de otros dispositivos administrados por el departamento de TI de la empresa RELIANCE.

CANTIDAD	DISPOSITIVO
1	Proyector
3	Impresora matricial
1	Impresora a tinta
1	Impresora multifuncional
1	Modem
1	Switch
1	UPS

Tabla 1.2: Otros Dispositivos Administrados por el Departamento de TI

1.2.2.4. SERVICIOS DE INTERNET Y BASE DE DATOS

Internet: El servicio de internet es proporcionado por INTERACTIVE, y es distribuido en la compañía sólo a las áreas gerenciales que son Gerencia y Dirección.

Base de Datos: El acceso a la base de datos esta dado mediante permisos y los ejecutivos de las áreas pueden acceder a realizar las consultas.

Red: Lo que se puede mencionar sobre la red de la compañía es; la topología de red que utiliza la empresa es del tipo estrella con conexiones punto a punto.
EL cableado que conforma la red es en parte por cable coaxial y el resto por cable UTP CAT 5e., el cable coaxial está entre el proveedor y el modem, para el del cableado estructurado se usa cable UTP. Adicionalmente cuentan con un Switch que permite establecer la conexión entre las maquinas que conforman la intranet de la compañía.

Como se puede observar en la Figura 1.2, el modem del proveedor de internet que para la compañía es INTERACTIVE se conecta al servidor, no todas las maquinas tienen acceso a internet ya que no lo requieren únicamente gerencia y dirección, este control se lo realiza mediante el Active Directory que también está instalado en el servidor, continuando con la red este servidor luego se conecta a un Switch al mismo que todas las demás se conectan estableciendo de esta forma la red.

No se cuenta con un firewall, solo está el antivirus corporativo de la institución como medio de seguridad de intento de hacking.

1.2.3. DESCRIPCIÓN DE LOS SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TI

En la Tabla 1.3 se describe los servicios que soporta el departamento de TI de la empresa RELIANCE.

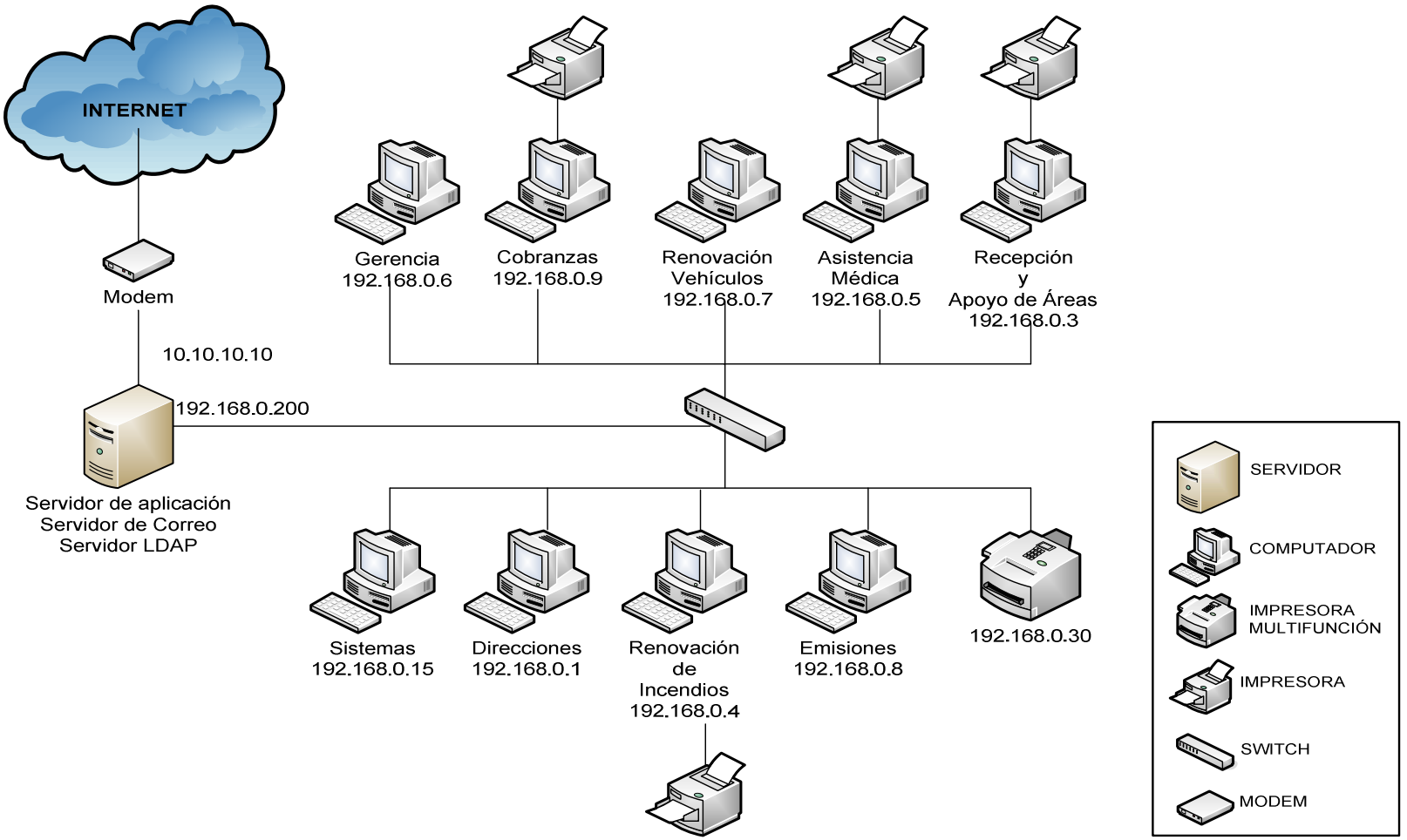

Figura 1.2: Topología de Red de RELIANCE[3]

[3] Autores: Javier Baños, Pamela Carrera, Gerente de Sistemas de RELIANCE (Santiago Granda)

SERVICIO DE TI	DESCRIPCIÓN
Microsoft Office	Suite de oficina con aplicaciones de procesamiento de textos, plantilla de cálculo y programa para presentaciones.
Outlook Express	Aplicación de cliente de correo electrónico usado para la recepción y envío de correo electrónico tanto a nivel interno de la empresa como externo a la misma.
Internet	Red pública que permite la conexión con otras redes y usada la comunicación, búsqueda y transferencia de información. Esta red es provista por la empresa INTERACTIVE.
Scanner	Captura y digitalización de imágenes, documentos de texto y transferencia de los mismos a un ordenador.
Impresora	Presentación de información impresa en papel, tanto texto como gráficos.
Fotocopiadora	Copiado en papel de un documento impreso.
Fax	Servicio utilizado para la transmisión y recepción de documentos mediante la red telefónica.
UPS	Sistema de alimentación de energía ininterrumpida, que permite proporcionar energía a un dispositivo en el caso de interrupción eléctrica.
SIBROK (Sistema Integrado de Brokers)	Sistema integrado que permite gestionar y administrar toda la información de las pólizas de seguros.
Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
Correo Electrónico	Servicio de red que permite a los usuarios enviar y recibir mensajes electrónicos, así como también enviar y recibir archivos. Este servicio es brindado por INTERACTIVE.
Servidor de Archivos	Servidor que permite el acceso remoto a archivos almacenados en el mismo o directamente accesibles por este.
Antivirus	Aplicación informática que permite prevenir, detectar y eliminar virus informáticos.

SERVICIO DE TI	DESCRIPCIÓN
Adobe Reader	Aplicación que permite abrir, guardar, imprimir y compartir documentos electrónicos.
Enlaces de Cableado	Red con cableado estructurado
Equipos de Computación y Componentes	Dispositivos eléctricos, electrónicos que permiten automatizar las tareas dentro de la organización, esto incluye a los dispositivos de almacenamiento extraíbles.
Acceso y Control Remoto (VNC)	Aplicación de control y asistencia remota a los usuarios de la empresa.
Proyector	Dispositivo que permite visualizar diapositivas proyectadas sobre una superficie lisa y regularmente usada para conferencias.

Tabla 1.3: Servicios que da soporte el Departamento de TI[4]

1.2.4. MAPEO DE SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TI A LAS AÉREAS DEL NEGOCIO

En la Tabla 1.4 se muestra los servicios que soporta el departamento de TI de RELIANCE por áreas del negocio.

DEPARTAMENTO	SERVICIO DE TI	
Gerencia	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Internet	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	

[4] Autores: Javier Baños, Pamela Carrera, Gerente de Sistemas de RELIANCE (Santiago Granda)

DEPARTAMENTO	SERVICIO DE TI	
Gerencia	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
	Proyector	
Dirección	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Internet	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	
	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	

DEPARTAMENTO	SERVICIO DE TI	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
	Proyector	
Emisión	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	
	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
Renovación	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	

DEPARTAMENTO	SERVICIO DE TI	
	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
Cobranzas	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	
	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	

DEPARTAMENTO	SERVICIO DE TI	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
Asistencia Médica	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	
	SIBROK	• Formularios • Reportes • Consultas
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	VNC	
Recepción	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	

DEPARTAMENTO	SERVICIO DE TI	
	UPS	
	Correo Electrónico	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
Sistemas	Microsoft Office	• Word • Excel • Power Point
	Outlook Express	
	Scanner	
	Impresora	
	Fotocopiadora	
	Fax	
	UPS	
	SIBROK	• Formularios • Reportes • Consultas • Ingreso de Datos • Depuración de Información
	Intranet	Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo.
	Correo Electrónico	
	Servidor de Archivos	
	Antivirus	
	Adobe Reader	
	Enlaces de Cableado	
	Equipos de Computación y Componentes	
	VNC	

Tabla 1.4: Mapeo de Servicios[5]

[5] Autores: Javier Baños, Pamela Carrera, Gerente de Sistemas de RELIANCE (Santiago Granda)

1.2.5. LISTADO DE LOS PROCESOS DEL DEPARTAMENTO DE TI

En la Tabla 1.5 se muestra la lista de procesos del departamento de TI de la empresa RELIANCE.

PROCESO DE TI	DESCRIPCIÓN	PERIODICIDAD
Creación de usuarios	Proceso encargado de registrar a los ejecutivos en Active Directory.	Cada vez que ingresa un ejecutivo a la compañía.
Obtención de Backus	Obtención de copias de seguridad de la información almacenada en la base de datos del sistema	Semanal
Mantenimiento de comunicaciones	Mantenimiento encaminado a mantener el funcionamiento óptimo de instalaciones y equipos de comunicación.	Semestral
Mantenimiento de hardware	Conjunto de acciones que tienen como objetivo mantener en estado óptimo el funcionamiento de los equipos de computación.	Trimestral
Mantenimiento de software	Procedimientos y medidas que permiten mantener el correcto funcionamiento de las diferentes aplicaciones de oficina utilizadas por las áreas de la empresa.	Diario
Adquisición de equipos	Proceso encargado de la elaboración de solicitudes de propuesta para la adquisición de nuevos equipos informáticos, así como el asesoramiento para la adquisición de los mismos.	Cada vez que un equipo es dado de baja o se requiere algún nuevo equipo.
Adquisición de Software	Proceso encargado de la elaboración de solicitudes de propuesta para la adquisición de nuevos paquetes de software que permitan automatizar las actividades de cada área de la empresa.	Depende del presupuesto anual aceptado por la empresa.
Soporte a usuarios	Proceso encargado de ayudar a satisfacer las necesidades de los usuarios con respecto a la correcta utilización de los equipos de TI tanto a nivel de hardware y software.	Diario

PROCESO DE TI	DESCRIPCIÓN	PERIODICIDAD
Capacitación de Usuarios	Capacitación realizada a nivel de software usado dentro de RELIANCE.	Depende del ingreso de nuevo personal, así como del uso de nuevas aplicaciones de software.
Mantenimiento y soporte del sistema SIBROK	Proceso encargado de asegurar que la información administrada por el sistema SIBROK sea precisa, consistente y esté disponible a los usuarios cuando estos lo necesiten y en la forma requerida para cada área de trabajo en RELIANCE.	Diario
Manejo de Cableado y equipos electrónicos	Proceso encargo de administrar el cableado de la red, así como de los equipos electrónicos de la empresa.	Semestral
Elaboración de reportes de producción	Proceso encargado de consolidar los reportes de las diferentes áreas para ser presentado a Dirección a final de mes.	Mensual
Ingreso de pólizas de seguro	Proceso encargado de ingresar toda la información de las pólizas de seguros a la base de datos del sistema.	Diario
Renovación de seguros	Proceso permite validar, renovar y actualizar los datos de las pólizas de seguro de los clientes asegurados.	Diario
Depuración de la información	Proceso encargado de validar toda la información que es enviada por el Banco.	Mensual

Tabla 1.5: Listado de Procesos del Departamento de TI[6]

[6] Autores: Javier Baños, Pamela Carrera, Gerente de Sistemas RELIANCE (Santiago Granda)

1.3. NECESIDAD DE LA DISPONIBILIDAD DE TI PARA LA EMPRESA RELIANCE

RELIANCE al ser una empresa en crecimiento y con visón hacia el futuro se ve en la necesidad de disponer de disponibilidad, fiabilidad, mantenibilidad y capacidad del servicio de TI para optimizar y monitorizar los servicios de TI, los cuales permitirán a la empresa gestionar y automatizar los procesos del negocio.

A continuación se indican los principales factores que requiere RELIANCE en la disponibilidad de TI:

- Reducir costos de operación y de adquisición de TI.
- Optimizar y monitorizar los servicios de TI.
- Incrementar la disponibilidad de los sistemas minimizando los riesgos de caída.
- Incrementar la calidad y satisfacción de los usuarios.
- Incrementar la agilidad de TI para adaptarse a los cambios y requerimientos constantes del negocio.
- Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios.
- Elaborar informes de seguimiento con la información recopilada sobre disponibilidad, fiabilidad, mantenibilidad y cumplimiento de servicios de TI.
- Mejorar la infraestructura y servicios TI con el objetivo de aumentar los niveles de disponibilidad.
- Disponer de planes y documentos que permitan gestionar la disponibilidad de TI a corto y medio plazo.

1.4. BENEFICIOS, COSTOS Y PROBLEMAS DE LA INDISPONIBILIDAD

1.4.1. BENEFICIOS DE LA DISPONIBILIDAD

A continuación se describen los beneficios que se obtiene de la Gestión de Disponibilidad:

- Se determina un responsable del diseño y monitoreo de la disponibilidad de los servicios de TI en la organización.
- Permite diseñar los servicios de manera que satisfagan los requerimientos de Disponibilidad en relación al negocio.
- Se establecen niveles de Disponibilidad los mismos que se miden y monitorizan permitiendo detectar fallos y cambios necesarios.
- Se detectan oportunamente caídas en la provisión de los servicios y se implementan medidas correctivas adecuadas
- Se disminuye la frecuencia y duración de los fallos con el pasar del tiempo.
- Se asegura una utilización y rendimiento adecuados de la infraestructura de TI para obtener los máximos beneficios mediante la consideración de los requisitos del negocio y los usuarios de los servicios.
- Se adopta una actitud proactiva en la organización TI, es decir, se pasa de una corrección de errores a una mejora continua en los servicios.
- Se observa el valor agregado que TI brinda al negocio.

1.4.2. COSTOS DE LA DISPONIBILIDAD

Entre los principales costos de la disponibilidad se pueden mencionar los siguientes:

- Costos de personal del proceso del proceso de Gestión de la Disponibilidad; sueldos, capacitación, consultoría externa de ser necesario.
- Costos de hardware, para las herramientas de monitoreo que se empleen.
- Costos de despliegue del diseño e implementación de los procesos, procedimientos y técnicas personalizadas al negocio.
- Costo de herramientas para la monitorización, análisis y realización de informes técnicos y ejecutivos.

1.4.3. PROBLEMAS DE LA INDISPONIBILIDAD

Entre los posibles problemas por la indisponibilidad se encuentran los siguientes:

- Falta de Disponibilidad de recursos.
- Falta de herramientas para la Gestión de la Disponibilidad.
- Falta de informes y reportes de disponibilidad.
- Falta de madurez en los procesos del negocio, para determinar las entradas y salidas claves para la gestión de la disponibilidad.

CAPÍTULO 2. PROCESO PARA LA ELABORACIÓN DEL PLAN DE DISPONIBILIDAD

En el presente capítulo se describe el proceso y las actividades que se deben seguir para la elaboración del Plan de Disponibilidad de Tecnologías de la Información (TI), para pequeñas y medianas empresas.

El presente proceso está de acuerdo a la Gestión de la Disponibilidad de TI, descrito en la librería de ITIL.

Las actividades descritas en este capítulo para el desarrollo del Plan de Disponibilidad de TI son las siguientes:

- Determinación de Requisitos de Disponibilidad
- Diseño de la Disponibilidad
- Diseño de la Recuperación
- Consideraciones de Seguridad
- Mantenimiento del Plan de Disponibilidad

2.1. DETERMINACIÓN DE REQUISITOS DE DISPONIBILIDAD

Los Requisitos de Disponibilidad son la base para estimar la capacidad del diseño de la Infraestructura de TI y el soporte que la organización de TI debe proporcionar para satisfacer las necesidades de Disponibilidad del negocio.

Antes de establecer los Requisitos de Disponibilidad de TI del negocio se consideran las siguientes actividades:

- Análisis de Impacto en El Negocio (BIA)
- Funciones Vitales del Negocio
- Requisitos de Disponibilidad

2.1.1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

El Análisis de Impacto en el Negocio permite identificar el impacto que produciría la indisponibilidad de los servicios de TI en las actividades del negocio.

En el Análisis de Impacto en el Negocio se debe desarrollar los siguientes aspectos:

- Objetivos y Alcance
- Identificación de Funciones y Procesos del Negocio
- Evaluación de Impacto Financiero y Operacional
- Identificación de Procesos Críticos del Negocio
- Identificación de Sistemas y Aplicaciones Críticas de TI
- Identificación de Tiempos máximos de Caída (MTD)
- Identificación del Tiempo Objetivo de Recuperación (RTO) y del Tiempo de Recuperación de Trabajo (WRT)
- Identificación del Objetivo de Punto de Recuperación (RPO)
- Análisis del daño a consecuencia de la interrupción de un servicio de TI

2.1.1.1. OBJETIVOS, ALCANCE DEL BIA

Objetivos: Establecer las metas relacionadas con el negocio, las cuales se alcanzaran mediante el desarrollo del BIA.

Alcance: Determinar a cual organización está dirigida el desarrollo del BIA, así como también determinar las limitaciones del BIA dentro de la organización.

2.1.1.2. IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DEL NEGOCIO

En esta sección se identifican todas las funciones y procesos del negocio.

Funciones: Son todas las áreas que constituyen la organización. Estas áreas son consideradas en el plan de disponibilidad:

Procesos: Es el conjunto de actividades organizadas que permite a los empleados de la organización realizar sus tareas, de acuerdo al área a la que pertenecen.

2.1.1.3. EVALUACIÓN DE IMPACTO FINANCIERO Y OPERACIONAL

En esta sección se evalúa el impacto financiero y operacional de los procesos de la organización.

2.1.1.3.1. EVALUACIÓN DEL IMPACTO FINANCIERO

El impacto financiero deberá ser evaluado de forma cualitativa en todos los casos, esto se debe a que las cifras reales son consideradas como información confidencial para cada organización.

Para la Evaluación del Impacto Financiero se debe de tener como precedente a la siguiente pregunta: ¿Cuál será la magnitud del impacto de pérdida financiera si los procesos del negocio fuesen interrumpidos?

Entre los factores que tienen que ser considerados para realizar la evaluación del impacto financiero son los siguientes

- Costos financieros
    - Reducción en los ingresos
    - Reducción de ganancias
    - Pérdida de un activo
    - Pérdida de producción
    - Incremento en los costos
    - Multas
- Costos no financieros
    - Pérdida de credibilidad

- Requisitos legales, regulatorios y seguridad

2.1.1.3.2. EVALUACIÓN DEL IMPACTO OPERACIONAL

En este punto se procederá a clasificar, identificar y a evaluar el impacto negativo que tendría la organización debido a la indisponibilidad de los servicios de TI.

Entre los factores que generan el Impacto Operacional, están los siguientes:

- Falta de confiabilidad operacional de:
  - Equipos de TI
  - Recursos humanos
  - Procesos
  - Mantenibilidad de los equipos
- Suficiencia del servicio prestado
- Eficacia del servicio
- Satisfacción del cliente
- Posicionamiento en el mercado
- Confianza del cliente
- Control de la compañía
- Ética
- Moral, etc.

La ponderación considerada para el análisis operativo de la entidad se basa directamente al grado de magnitud de impacto que afectaría en la proyección como: Flujo de Caja, Participación de Mercado, Competitividad, satisfacción del Cliente.

2.1.1.4. IDENTIFICACIÓN DE PROCESOS CRÍTICOS DEL NEGOCIO

En esta etapa se identifican los procesos críticos del negocio, los cuales en una ocurrencia de un hecho o incidente pueden:

- Discontinuar la marcha de las operaciones del negocio.
- Afectar a la calidad de servicio que se otorga al cliente.
- Retrasar las actividades y tareas del personal de la organización.
- Afectar negativamente en el Flujo de Caja, Satisfacción del Cliente y la Consolidación de la Organización en el Mercado.

Para poder definir los procesos críticos del negocio se procede a analizar los resultados obtenidos en la etapa anterior, con respecto al análisis de impacto financiero y de impacto operacional.

Un proceso será considerado como crítico si:

- En el Impacto Financiero se obtuvo un valor de 2 o 3.
- Si en el Impacto operacional existen al menos dos valores “Alto”.
- Si en el Impacto Operacional existen al menos un valor “Alto” y un valor “Medio”.

2.1.1.5. IDENTIFICACIÓN DE SISTEMAS Y APLICACIONES CRÍTICAS DE TI POR PROCESO DEL NEGOCIO

Los sistemas y aplicaciones críticas de TI son aquellas que soportan procesos críticos del negocio, es decir todo proceso de la empresa que involucre servicios de TI. Por tanto, a estos procesos se los considera como procesos críticos del Departamento de TI.

2.1.1.6. IDENTIFICACIÓN DE TIEMPOS MÁXIMOS DE CAÍDA (MTD)

Entre los objetivos de BIA, es determinar un común acuerdo de cuáles son los máximos tiempos tolerables de caída (MTD), para cada uno de los recursos críticos del negocio. Con los MTD se trata de lograr tener valores cuantitativos con relación al impacto financiero que un evento adverso pueda tener sobre la organización o una división de esta misma.

Para identificar a los MTD's, se procede a utilizar el total de puntos obtenidos de la suma resultante entre el Impacto Financiero y el Impacto Operacional.

2.1.1.7. IDENTIFICACIÓN DEL TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) Y DEL TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT)

En esta etapa se determinan el tiempo que se requerirá disponer de un servicio, el cual ha estado fuera de operación, y que por tanto impide la continuidad y disponibilidad de las actividades del negocio. La duración de este tiempo inicia en el momento en que el servicio de TI esta fuera de operación, hasta que se lo logre nuevamente poner en funcionamiento.

2.1.1.7.1. TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)

"El RTO (Recovery Time Objective) es el Tiempo objetivo de recuperación, en otras palabras cuanto puede permanecer la Organización sin ejecutar una actividad, el uso de una aplicación (hardware y/o software) o información relevante. Frecuentemente es asociado con el tiempo máximo de inactividad. El RTO se utiliza para decidir cada cuanto se deben realizar respaldos de información o backups; también es útil para decidir que infraestructura es requerida para reiniciar operaciones, por ejemplo un centro de cómputo alterno de similares especificaciones al existente en la Organización, o un callcenter paralelo en una ubicación diferente a la que se utiliza de manera permanente."[7]

2.1.1.7.2. TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT)

El WRT indica el tiempo que se requerirá para la recuperación de los datos que se han perdido durante la jornada laboral, trabajo retrasado y todos aquellos datos

[7]Camelo, Leonardo. Análisis de Impacto de Negocios / Business Impact Analysis (BIA). http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html, 30-05-2010

que han sido capturados de forma manual, una vez que los servicios de TI han sido recuperados después de estar fuera de servicio.

2.1.1.7.3. EVALUACIÓN DE RTO Y WRT

Para la evaluación de los tiempos de RTO, primero se toma en cuenta la recuperación de los sistemas y recursos críticos de área de TI, debido a que los servicios que provee esta área son considerados como actividades bases, las cuales permiten poner en marcha las demás actividades del negocio. La escala para el RTO se la determina en función del tiempo.

Los valores de WRT se evaluarán para los servicios de TI que almacenen datos, tal como es el caso de los sistemas y aplicaciones.

2.1.1.8. IDENTIFICACIÓN DEL OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO)

El RPO (Recovery Point Objetive) es el Objetivo de Punto de Recuperación, el cual se define como: “La cantidad máxima de información que puede ser pérdida cuando el o los servicios de TI es o son restaurados tras una interrupción. El Objetivo de Punto de Recuperación se expresa como una longitud de tiempo antes del Fallo. Por ejemplo, un Objetivo de Punto de Recuperación de un día debe ser soportado por Copias de Seguridad diarias, y hasta 24 horas de información pueden ser pérdidas.”[8]

2.1.1.9. ANÁLISIS DEL DAÑO A CONSECUENCIA DE LA INTERRUPCIÓN DE UN SERVICIO DE TI

En esta sección se determinan las consecuencias que se darían a causa de la interrupción de un servicio o recurso de TI.

[8] Centro Cristológico Nacional (España), Objetivo del Punto de Recuperación, https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/o/rpo.htm, 24-09-2009

2.1.2. FUNCIONES VITALES DEL NEGOCIO

Las Funciones Vitales del Negocio son todas en las que se tiene procesos críticos y determinan el éxito del Negocio.

Los criterios empleados para determinar los procesos críticos son los siguientes:

- En el Impacto Financiero se obtuvo un valor de 2 o 3.
- Si en el Impacto operacional existen al menos dos valores “Alto”.
- Si en el Impacto Operacional existen al menos un valor “Alto” y un valor “Medio”.

2.1.3. REQUISITOS DE DISPONIBILIDAD

En esta sección del documento se proporciona la base para estimar la capacidad del diseño de la Infraestructura de TI y el soporte que la organización de TI debe proporcionar para satisfacer las necesidades de Disponibilidad del negocio.

Para plantear los requisitos del negocio de Disponibilidad de TI se considera lo siguiente:

- Una definición de las funciones vitales para el negocio que dependan de los servicios TI.
- Una definición del tiempo de caída del servicio TI, esto es, las condiciones bajo las cuales el negocio considera que el servicio TI no está disponible.
- El impacto sobre el negocio causado por la pérdida del servicio.
- Los requisitos de Disponibilidad cuantitativos, esto es, el grado en que el negocio puede tolerar una caída del servicio TI o un servicio degradado.
- Las horas de servicio necesarias, esto es, cuándo se va a proporcionar el servicio.
- Una evaluación de la importancia relativa de los diferentes periodos de trabajo.
- Las necesidades de seguridad específicas.

2.1.3.1. ALCANCE

En esta sección del documento se describe cada servicio de TI de la organización.

2.1.3.2. RESUMEN DE DISPONIBILIDAD DE SERVICIO TI

En este punto del documento se representa un resumen de los servicios TI con los siguientes criterios:

- Encargado de TI del servicio
- Horas de Servicio
- Tiempo de Recuperación Capacidad de Adaptabilidad
- Utilidad
- Periodo de Mantenimiento

2.1.3.3. REQUERIMIENTOS DE DISPONIBILIDAD

En esta sección se describe los requerimientos de cada uno de los servicios de TI de la organización, para lo cual se toma como referencia los siguientes criterios:

- Nombre del Servicio
- Descripción del Servicio
- Requerimientos del Negocio
- Fallos
- Funciones Vitales Relacionadas con este Servicio

2.2. DISEÑO DE LA DISPONIBILIDAD

“El diseño de la disponibilidad es una actividad proactiva orientada a evitar la pérdida de la disponibilidad de los servicios de TI. Esta actividad está relacionada con el diseño técnico de la Infraestructura de TI y con la alineación de los

proveedores internos y externos necesarios para satisfacer las necesidades de Disponibilidad de un servicio de TI.

Mediante el Diseño de la Disponibilidad se reducirá la posibilidad de:

- Incremento de los costos de desarrollo de tener que volver a realizar tareas ya ejecutadas.
- Afrontar gastos imprevistos en actualizaciones, necesarias para satisfacer los requisitos de Disponibilidad.
- Afrontar gastos innecesarios en herramientas adicionales de Gestión de Sistemas, necesarios para controlar y gestionar el funcionamiento de los servicios de TI y de la Infraestructura de TI que los mantiene.
- Prevenir retrasos en la planificación prevista y la posibilidad de perder oportunidades de negocio.
- Incurrir fallos del servicio evitables."[9]

A continuación se indica las actividades a desarrollarse en la etapa del Diseño de la Disponibilidad:

- Diseño de la infraestructura TI.
- Análisis de Puntos Individuales de Fallo de Componentes (SPOF).
    - Análisis de Impacto del Fallo de Componentes (CFIA).
    - Análisis por Arboles de Fallos (FTA).
- Gestión y Análisis de Riesgo.

2.2.1. DISEÑO DE LA INFRAESTRUCTURA TI

La Infraestructura TI es la suma de todos los componentes de hardware, software y servicios profesionales necesarios para hacer funcionar las múltiples aplicaciones de tecnología de información, y que permite a la organización apoyar y automatizar los procesos del negocio.

[9] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

A pesar de que la infraestructura TI es importante, las organizaciones quieren invertir pocos fondos en este rubro, dado que esta inversión no tiene una tasa de retorno de fácil medición.

Para el diseño de la Infraestructura TI, se utilizan los elementos de configuración (CI).

El propósito de esta sección, es realizar recomendaciones para el mejoramiento de la existente infraestructura TI, contando con los elementos ya disponibles por parte de la organización, y con sugerencias en la incorporación de nuevos elementos tanto de hardware, software y técnicas, que permitan la de disponibilidad de servicios de TI.

2.2.1.1. ELEMENTOS DE LA RED

Todos los elementos descritos en este punto permitirán la posibilidad de ingresar electrónicamente desde puntos locales y remotos a recursos de red, plataformas de impresión, bases de datos y aplicaciones críticas de negocio, brindando al usuario un mayor soporte, control y disponibilidad de los servicios de TI, de manera segura y confiable.

Los beneficios que ofrecen los recursos de red a los usuarios son los siguientes:

- Calidad y rapidez de servicio a clientes al acceder a sus sistemas desde puntos remotos
- Tecnología para crear estaciones de trabajo móviles, evitando duplicidades y costo adicional
- Seguridad, confidencialidad e integridad de la información durante tus operaciones
- Realizar consultas y transacciones desde puntos remotos.

2.2.1.2. ADMINISTRACIÓN DE TI

Es el conjunto de herramientas que nos permiten controlar en una infraestructura de TI, diversos aspectos como: activos, inventarios y distribución centralizada de software, prevención de riesgos de fallas, etc. a través de una consola principal.

Los beneficios que se obtienen con los elementos de administración de TI son los siguientes:

- Preservación de activos
- Anticipación de caídas de sistemas
- Ahorro de tiempo al distribuir software de manera centralizada
- Productividad al verificar que el software cargado en los clientes corresponda a su función.
- Administración de plataformas de hardware y software.

2.2.1.3. ALMACENAMIENTO

Son todas aquellas herramientas de respaldo, disponibilidad y preservación de la información que permiten salvaguardar el activo vital de la organización, así como, procurar la continuidad y competitividad del negocio.

Los beneficios que se obtienen con los componentes de almacenamiento son los siguientes:

- Protección e Integridad de la información del negocio.
- Posibilidad de respaldos en línea y automáticos.
- Disponibilidad de información en caso de contingencia.

2.2.1.4. IMPRESIÓN Y DIGITALIZACIÓN

Son todos aquellos equipos y herramientas de captura, digitalización y presentación de información impresa en papel.

Los beneficios que se obtiene con los componentes de impresión y digitalización son los siguientes:

- Disponibilidad de contratos, solicitudes, memorándums, respaldos físicos, que permiten una manipulación más directa con el usuario.
- Posibilidad de tener una copia digitalizada de los documentos físicos de alta importancia.
- Disminución del espacio físico de almacenamiento de información.

2.2.1.5. CONSIDERACIONES PARA EL HARDWARE Y SOFTWARE

2.2.1.5.1. CONSIDERACIONES DE HARDWARE

En este punto se describirán las característica mínimas necesarias que deberán tener los equipos informáticos a nivel de hardware, para mantener la disponibilidad de los servicios TI.

2.2.1.5.2. CONSIDERACIONES DE SOFTWARE

En este punto se describirán las característica mínimas necesarias que deberán tener las aplicaciones y herramientas de software, para mantener la disponibilidad de los servicios TI.

2.2.1.6. CONSIDERACIONES PARA EL ENTORNO DE LA INFRAESTRUCTURA DE TI

En la esta sección se detalla la arquitectura y estándares para el entorno de la Infraestructura de TI.

2.2.2. ANÁLISIS DE PUNTOS INDIVIDUALES DE FALLO DE COMPONENTES (SPOF)

"Un Punto Único de Fallo es cualquier componente de la Infraestructura TI del que no se tenga "Competencia de backup", y cuyo fallo pueda tener un impacto negativo sobre el negocio y los usuarios.

Es importante que en el diseño de la Infraestructura TI no exista ningún punto individual de fallo sin localizar, por lo que se utiliza para la identificación de estos puntos únicos de fallos a la técnica "Análisis del Impacto del Fallo de un Componente (CFIA)""[10].

2.2.2.1. ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE (CFIA)

En esta sección se procede a determinar el impacto sobre la Disponibilidad del servicio de TI, derivada de los fallos de los componentes incluidos en la Infraestructura TI, y el diseño de los servicios que han sido propuestos.

"El desarrollo del CFIA nos proporciona:

- Puntos individuales de fallo que puedan impactar sobra la disponibilidad de TI.
- Impacto del fallo de un componente sobre la operativa del negocio y los Usuarios.
- Dependencia del personal y los componentes.
- Tiempos de recuperación de los componentes.
- Identificar y documentar las opciones de recuperación.
- Identificar e implementar medidas de reducción del riesgo."[11]

Para la realización del CFIA se procede a utilizar la Infraestructura TI propuesta anteriormente, donde el primer paso será crear un diagrama con los Elementos de Configuración (CI) en un eje y los servicios que dependen de cada CI en el otro.

---

[10] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

[11] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

A continuación se realiza el siguiente procedimiento para cada punto de intersección que se ha determinado:

- Se deja un espacio en blanco, cuando el fallo del CI no impacta de ningún modo sobre el servicio.
- Se coloca una X cuando el fallo del CI provoca la inoperatividad del servicio.
- Se coloca una A cuando existe un CI alternativo que pueda proporcionar el servicio.
- Se coloca una B cuando existe un CI alternativo, pero primero se debe de recuperar el servicio.

Finalmente se debe realizar una matriz que representa a los Elementos de Configuración, y el efecto que produce en las diferentes áreas del negocio, y el total de usuarios que son afectados por la pérdida de servicios de TI, que ofrecen estos Elementos de Configuración.

2.2.2.2. ANÁLISIS POR ARBOLES DE FALLOS (FTA)

“El Análisis del Árbol de Fallos (FTA) es una técnica que se utiliza para determinar la cadena de sucesos que causa una interrupción de los servicios de TI. Esta técnica, junto con la utilización de métodos de cálculo, ofrece modelos de Disponibilidad detallados.

Las ventajas fundamentales del FTA son:

- Permite realizar cálculos de la Disponibilidad.
- Permite realizar las operaciones sobre el árbol de fallos resultante, estas operaciones corresponde con cada una de las opciones del diseño.
- Permite elegir el nivel deseado de detalle del análisis.

Para el desarrollo del FTA, se distingue los siguientes sucesos:

- Sucesos Básicos: Puntos terminales del árbol de fallo, como la perdida de suministro eléctrico o un error del operador. Los sucesos básicos no se investigan con más profundidad. Si los sucesos básicos se investigan con más profundidad, automáticamente se convierten en sucesos resultantes.
- Sucesos Resultantes: Nodos intermedios del árbol de fallos que resultan de una combinación de sucesos. Habitualmente, el punto superior del árbol de fallos es el fallo del servicio TI.
- Sucesos Condicionados: Sucesos que solo ocurren bajo ciertas condiciones, como por ejemplo, el fallo del equipo de aire acondicionado solo afectara al servicio TI si la temperatura de los equipos supera los valores de servicio.
- Sucesos Desencadenantes: Sucesos que lanzan otros sucesos, por ejemplo, el equipo de detección de la pérdida del suministro eléctrico puede lanzar el cierre automático de servicios TI.

Estos sucesos se combinan mediante operadores lógicos, como:

- AND: El evento resultante solo sucede cuando todos los sucesos entrantes ocurren simultáneamente.
- OR: El evento resultante ocurre cuando suceden uno o más de los eventos entrantes.
- OR exclusivo: El evento resultante solamente ocurre cuando se satisface la condición de entrada.
- Inhibidor: El evento resultante solamente ocurre cuando no se satisface la condición de entrada".[12]

2.2.3. GESTIÓN Y ANÁLISIS DE RIESGO

En esta sección se procede a evaluar la vulnerabilidad a los fallos de la configuración y la capacidad de la organización TI, por lo tanto, se procede a realizar un análisis del riego formal a las configuraciones y diseño de los servicios,

[12] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

y a las organizaciones que los mantiene (proveedores internos y externos). Para este análisis se utiliza el método CRAMM (Método de Análisis y Gestión de Riesgos), la cual es una técnica que permite identificar las contramedidas justificables que pueden proteger la Disponibilidad de los servicios TI.

"***Análisis del Riesgo:*** Identifica y determina el nivel de (medida) los riesgos calculados a partir de los valores estimados de los activos y los valores estimados de las amenazas y las vulnerabilidades de tales activos.

Gestión del Riesgo: Cubre la identificación, selección y adopción de contramedidas justificadas por los riesgos identificados para los activos en términos de su impacto potencial sobre los servicios si ocurriera un fallo, y la reducción de tales riesgos a un nivel aceptable."[13]

En la Figura 2.1 se indica el análisis y la gestión del riesgo como dos actividades relacionadas pero separadas.

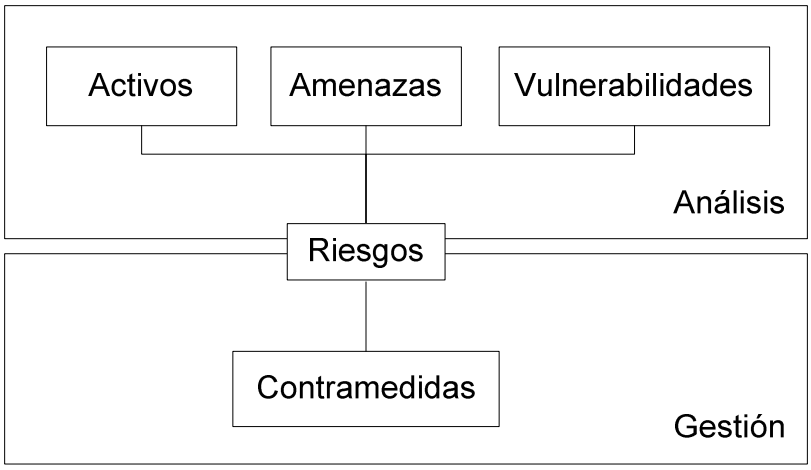

Figura 2.1: Análisis y Gestión de Riesgos[14]

[13] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

[14] Estructura de la figura tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

2.2.3.1. MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS (CRAMM)

En esta sección se procede a la identificación de los posibles riesgos que pueden afectar a la prestación de los servicios TI en la organización. También se desarrollan contramedidas justificadas para reducir o eliminar las amenazas de tales riesgos, todo esto con el fin de alcanzar niveles de Disponibilidad necesarios en la prestación de servicios TI.

El método de análisis y gestión de riesgos CRAMM, consta de las siguientes etapas:

- Valoración de los activos
- Identificación y valoración de las amenazas
- Identificación y valoración de vulnerabilidades
- Evaluación de los niveles de riesgo
- Opciones de control de riesgos

2.2.3.1.1. VALORACIÓN DE ACTIVOS

Los activos corresponden a cada uno de los componentes que son parte del proceso del negocio. Los activos pueden incluir a las personas, el alojamiento, sistemas informáticos, redes, registros en papel, máquinas de fax, etc.

2.2.3.1.2. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

"Una amenaza es la probabilidad de que un incidente no deseado pueda afectar a los procesos de la organización de alguna manera."[15]

[15] Compute-rs. Gestión de la Disponibilidad. http://www.compute-rs.com/es/search.php?search=cramm, 20-06-2010

2.2.3.1.3. IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES

"La Vulnerabilidad es una medida de cuán susceptible es un activo expuesto a ser afectado por un fenómeno perturbador."[16]

2.2.3.1.4. EVALUACIÓN DE NIVELES DE RIESGOS

"Un riesgo es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento."[17]

Para determinar el valor del riesgo se procede a tomar los valores de los activos y multiplicarlos por el valor de la probabilidad de las amenazas y también multiplicado por los valores de las vulnerabilidades.

2.2.3.1.5. OPCIONES DE CONTROL DE RIESGOS

A continuación se procede a determinar las posibles contramedidas para contrarrestar el efecto de un riesgo. También se determina las opciones de control de riesgo, las cuales se dividen en las siguientes categorías:

Aceptación del Riesgo: Consiste en aceptar el riesgo y no hacer nada.
Anulación del Riesgo: Consiste en anular el riesgo totalmente.
Reducción del Riesgo: Consiste en reducir el riesgo a niveles aceptables.
Transferencia del Riesgo: Consiste en transferir el riesgo a otra entidad u organización.

---

[16] Compute-rs. Gestión de la Disponibilidad.
http://www.compute-rs.com/es/search.php?search=cramm, 20-06-2010
[17] Villalva, Juan. Riesgos.
http://www.monografias.com/trabajos35/tipos-riesgos/tipos-riesgos.shtml, 20-07-2010

2.3. DISEÑO DE LA RECUPERACIÓN

La gestión de la disponibilidad debe asegurarse que en la actividad de diseño se centre en los componentes del servicio necesarios para garantizar que cuando fallen los servicios, se puedan retornar las operaciones normales del negocio tan rápidamente como sea posible.

Para obtener un buen diseño de la recuperación se deben considerar las necesidades a satisfacer del negocio (es la información que tienen de los clientes, productos y servicios) y las necesidades de la organización de TI (consisten en los procesos, procedimientos y herramientas necesarias para poder realizar la recuperación técnica en un tiempo óptimo) que permita la recuperación eficaz de los fallos.

Entre las actividades del Diseño de la Recuperación, constan las siguientes:

- Elementos principales del diseño de la recuperación
- Gestión de sistemas
- Captura de datos para el diagnostico
- Necesidades de recuperación y backup
- Métricas de recuperación

2.3.1. ELEMENTOS PRINCIPALES DEL DISEÑO DE LA RECUPERACIÓN

La gestión de la Disponibilidad tiene relación con la Gestión del Incidente y del Centro de Servicio al Usuario para asegurarse e eliminar la repetición de fallos similares. Para asegurar satisfacer las necesidades del negocio durante los fallos se debe haber definido y ejecutado:

- Unos estrictos procedimientos de reasignación de tareas
- Roles y responsabilidades claramente definidos para gestionar los incidentes más importantes
- Un plan de comunicaciones para cubrir el incremento de necesidades informativas, relacionado con los incidentes más importantes.

2.3.2. GESTIÓN DE SISTEMAS

La provisión de herramientas de gestión de sistemas influye positivamente sobre los niveles de disponibilidad que se pueden conseguir. Usar estas herramientas para proporcionar una detección automática de los fallos, ayudar con el diagnostico de los mismos y permitir realizar una recuperación automática.

2.3.3. CAPTURA DE DATOS PARA EL DIAGNOSTICO

Cuando falla un componente, es importante recopilar el nivel necesario de datos para el diagnóstico, a fin de permitir identificar la causa raíz del problema. Para algunos fallos, la captura de los datos para el diagnóstico puede ampliar el tiempo de caída del servicio. Sin embargo, no capturar los datos apropiados expone al servicio a una repetición de los fallos.

El tiempo empleado para la captura de datos no debe ser excesivo, se debe promover una revisión para determinar si se pueden perfeccionar las técnicas y/o procedimientos para reducir el diagnóstico y asegurar que sólo se capturan los datos que se consideran esenciales.

2.3.4. NECESIDADES DE RECUPERACIÓN Y BACKUP

En este punto se procede a listar las necesidades de recuperación y “backup” de los componentes en que se basan los servicios TI, estas necesidades contemplan el hardware, software y datos.

2.3.5. MÉTRICAS DE RECUPERACIÓN[18]

Proporcionar una estimación oportuna y exacta acerca de cuándo se restaurará el servicio ayuda al negocio para tomar decisiones razonables de cómo se pueden gestionar el impacto del fallo sobre el negocio y sobre sus clientes. Para poder proporcionar esta información al negocio se requiere crear y mantener unas métricas de la recuperación de cada componente TI que cubran una amplia variedad de escenarios diferentes.

Entre las métricas a considerar están las siguientes:

- Métricas de tiempo
- Métricas de costos
- Métricas de efectividad del plan de recuperación
- Restauración y comprobación del servicio

2.4. CONSIDERACIONES DE SEGURIDAD

El objetivo general de la seguridad TI es conseguir alcanzar una seguridad equilibrada con unos controles justificables, implementado para garantizar la continuidad del servicio TI dentro de unos parámetros seguros como son:

- Confidencialidad
- Integridad
- Disponibilidad

[18] Fuentes:

- Wikipedía. Plan de Recuperación ante desastres. http://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres, 30-07-2010
- IBM. Plan para la recuperación ante siniestros. http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzaj1/rzaj1disastr.htm. 20-07-2010
- Kirvan Paul. IT disaster recovery Plan template. http://searchdisasterrecovery.techtarget.com/generic/0,295582,sid190_gci1370683,00.html. 13-10-2009

Dentro de la Gestión de la Disponibilidad, la seguridad se encarga de garantizar que se definan e incorporen los requisitos y políticas de seguridad en el diseño general de la Disponibilidad.

Mediante la utilización del estándar británico **7799** "El código de prácticas británico para la seguridad de la información", y actualmente conocido como el Estándar Internacional **ISO/IEC 17799**, se procede a determinar los respectivos controles y políticas de seguridad para la empresa RELIANCE.

"Control: Es el medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas de gestión de o naturaleza legal. Los controles también se los utiliza como sinónimo de salvaguarda o contramedida.

Política de Seguridad: El objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes."[19]

2.4.1. SEGURIDAD DE LA INFORMACIÓN

El objetivo es manejar la seguridad de la información dentro de la organización, para lo cual las actividades deben de ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes. Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo.

[19] Organización Internacional para la Estandarización (ISO), Comisión Electrotécnica Internacional (IEC). Estándar Internacional ISO/IEC 17799. 2005

2.4.2. SEGURIDAD FÍSICA Y AMBIENTAL

El objetivo es evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados, por lo cual debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

2.4.3. SEGURIDAD DE LOS EQUIPOS

El objetivo es evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

2.4.4. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

El objetivo es asegurar la operación correcta y segura de los medios de procesamiento de la información.

2.4.5. RESPALDO O BACK-UP

El objetivo es mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

2.4.6. SEGURIDAD DE LA RED

El objetivo es asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

2.4.7. MONITOREO

El objetivo es detectar las actividades de procesamiento de información no autorizadas.

2.4.8. ROLES Y RESPONSABILIDADES

A continuación se describe el rol que interviene en el proceso de Administración de la Disponibilidad.

Administrador de Disponibilidad

Misión

Asegurar que se cumplan todas las políticas y procedimientos de la Administración de Disponibilidad.

Responsabilidades

- Asegurar el cumplimiento de los Disponibilidad
- Asegurar la mejora continua de los servicios
- Reportar servicios a la dirección
- Implementar nuevos servicios
- Auditar los servicios

Competencias

- Ingeniería en Sistemas o carrera afín y experiencia en la operación de TI
- Conocimiento y experiencia en tecnologías de información
- Conocimiento de las herramientas para la Administración de Disponibilidad
- Experiencia en la Administración de Negocios
- Fundamentos de ITIL o *Practitioner* en ITIL (Módulo *Availability*)
- Inglés 80%.

Habilidades

- Habilidades Administrativas

- Facilidad de palabra
- Capacidad de trabajo en equipo
- Conocimiento y experiencia en la infraestructura de la organización
- Conocimiento de la organización

2.5. MANTENIMIENTO DEL PLAN[20]

Uno de los resultados principales del proceso de Gestión de la Disponibilidad es la creación de un Plan de Disponibilidad, el cual debe ser a largo plazo para la mejora proactiva de la disponibilidad considerando las limitaciones de costo impuesto.

La mejora de la Disponibilidad viene dado por uno o varios de los siguientes motivos:

- La incapacidad de un nuevo servicio TI para satisfacer los SLA's.
- Periodos de inestabilidad del servicio TI que conllevan a unas niveles de Disponibilidad intolerables.
- Las tendencias de las mediciones de la Disponibilidad indican un deterioro gradual de la misma.
- Tiempos de recuperación y restauración del servicio TI inaceptables
- La solicitud de incrementar el nivel de disponibilidad ofrecido por la organización de TI.
- El impacto de los fallos de servicio TI al negocio y clientes causados por un incremento de la demanda del negocio.

La gestión de la disponibilidad debe desempeñar una función proactiva para identificar y promover las oportunidades de mejora de la Disponibilidad con las siguientes consideraciones:

[20] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

2.5.1. MONITORIZACIÓN Y ANÁLISIS DE LAS TENDENCIAS DE GESTIÓN DE LA DISPONIBILIDAD

Identificar y promover las oportunidades de mejora de la Disponibilidad justificables en términos de su costo, las mediciones apropiadas y significativas de la disponibilidad y los informes pertinentes apoyan a esta tarea.

2.5.2. DETERMINAR LOS REQUISITOS DE DISPONIBILIDAD (Modificados)

Cuando el negocio necesite una mejora de la disponibilidad, debe seguirse el proceso definido para reevaluar la capacidad de la infraestructura TI y de la organización TI para satisfacer este aumento de requisitos.

2.5.3. EL COSTO DE MEJORAR LA DISPONIBILIDAD

Satisfacer las necesidades del negocio con niveles de niveles de disponibilidad altos puede requerir una inversión financiera adicional para mejorar la Infraestructura TI y o ampliar los servicios que proporciona la organización TI. Se debe justificar el costo adicional con el costo de fallo de TI esto ayuda a tomar decisiones de realizar una inversión financiera. Sin embargo se debe recordar que uno de los objetivos de la Gestión de la disponibilidad es la oportunidad que ofrece para optimizar la disponibilidad de la Infraestructura de TI con un costo reducido.

2.5.4. MÉTODOS Y TÉCNICAS

Existe una serie de métodos y técnicas que se pueden utilizar para identificar las oportunidades de mejora de la disponibilidad.

Dentro de los que se tiene:

- El asesoramiento de impacto de impacto del fallo de un componente
- Análisis del árbol de fallos
- CRAMM

- Análisis de la interrupción del sistema
- El ciclo de vida de incidentes ampliado
- Mejora continua
- Puesto de observación técnica

CAPÍTULO 3. ELABORACIÓN DEL PLAN DE DISPONIBILIDAD DE TI PARA LA EMPRESA RELIANCE

En este capítulo se procede a la elaboración del Plan de Disponibilidad de TI, para la empresa RELIANCE. Este plan permitirá estructurar y reunir todas las iniciativas que pueden ser necesarias para mejorar la Disponibilidad de los servicios de TI, así como la infraestructura de TI actual de la organización.

La elaboración del Plan de Disponibilidad inicia con la descripción de todos los componentes necesarios para el desarrollo del proceso de la Gestión de la Disponibilidad.

Entre los componentes del proceso de Gestión de la Disponibilidad, primero se definen a las Actividades Vitales del Negocio, para lo cual se realiza un mapeo de las actividades de la organización por áreas, teniendo en cuenta a aquellas actividades que están o no relacionadas con las Tecnologías de la Información.

A continuación se procede a determinar los elementos de configuración que son aquellos componentes que definen a la infraestructura tecnológica actual de la organización.

Una vez definidos los componentes del proceso de Gestión de la Disponibilidad, se procede a la Determinación de Requisitos de Disponibilidad. Estos requisitos permitirán determinar las necesidades reales del negocio, con respecto a la Disponibilidad de las Tecnologías de la Información. También esta Determinación de Requisitos de Disponibilidad, permitirá evaluar si la Infraestructura de TI de la organización, puede proporcionar los niveles necesarios de Disponibilidad.

Una vez determinados los Requisitos de Disponibilidad del negocio, se procede a desarrollar la actividad de diseño. Esta actividad permitirá garantizar que se pueden satisfacer el nivel de disponibilidad requerido por los servicios de TI, que apoyan a las actividades del negocio, por lo tanto estas actividades de diseño son la clave de la Gestión de la Disponibilidad.

Las actividades de diseño son:

- El Diseño de la Disponibilidad
- El Diseño de la Recuperación
- Consideraciones Sobre la Seguridad
- Mantenimiento del Plan de Disponibilidad.

Las actividades del Diseño de la Disponibilidad y del Diseño de la Recuperación, son consideradas como actividades Proactivas y Reactivas respectivamente, donde estas actividades son parte del proceso de Gestión de la Disponibilidad.

A continuación en la Figura 3.1 se representa a las actividades Proactivas y Reactivas del Proceso de Gestión de la Disponibilidad que se van a desarrollar en este capítulo.

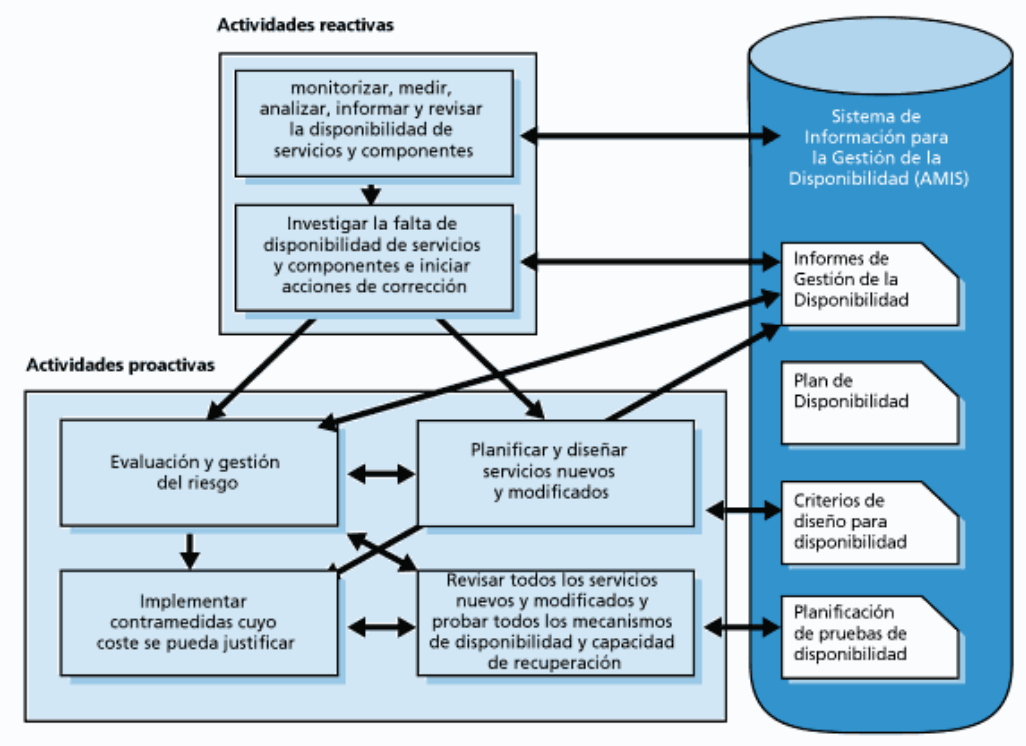

Figura 3.1: Procesos de la Gestión de la Disponibilidad[21]

Es necesario indicar que en este punto, también se desarrollaran todas las actividades requeridas para el desarrollo del Plan de Disponibilidad.

El Plan de Disponibilidad contendrá la siguiente información:

- La situación actual de disponibilidad de los servicios TI.
- Herramientas para la monitorización de la disponibilidad.
- Métodos y técnicas de análisis a utilizar.
- Definiciones relevantes y precisas de las métricas a utilizar.
- Planes de mejora de la disponibilidad.
- Expectativas futuras de disponibilidad.

3.1. ACTIVIDADES VITALES DEL NEGOCIO

A continuación se procede a identificar todas aquellas actividades necesarias para obtener resultados favorables, para que una empresa tenga funcionamiento exitoso, es decir se identifican los Factores Críticos de Éxito (FCE).

3.1.1. ACTIVIDADES DEL NEGOCIO RELACIONADAS CON TI

En la Tabla 3.1 se describen las principales actividades del negocio divididas por áreas y los servicios que TI les proporciona.

ÁREA	ACTIVIDAD RELACIONADA CON TI		RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SI	NO		
Emisión		X		Recepción de Solicitudes de Póliza.

[21] Office of Government Commerce (OGC); ITIL la Llave para la Gestión de los Servicios TI; Mejores Prácticas para la Provisión del Servicio; versión 3;2007

ÁREA	ACTIVIDAD RELACIONADA CON TI		RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SI	NO		
		X		Verificar información completa presentada en la Solicitud de Pólizas
	X		Microsoft Excel - Impresora	Emisión del certificado del seguro(5 copias)
	X		Correo Electrónico - Fax	Envío de certificados a Ejecutivos de Banco Promerica
	X		Correo Electrónico - Adobe Acrobat	Envío de certificado firmado a la compañía de seguros
	X		Correo Electrónico - Adobe Acrobat	Pedido de facturación a la compañía de seguros
	X		SIBROK - Microsoft Excel	Verificación de datos del certificado versus Factura
	X		SIBROK	Ingreso de facturas de listado de pagos de producción mensual
	X		SIBROK	Pago de primas acreditado a la cuenta de la compañía de seguros
Renovación	X		SIBROK - Correo Electrónico - Microsoft Excel	Generación de la base de datos de clientes con pólizas a vencer
	X		SIBROK - Correo Electrónico - Microsoft Excel	Validación de la información de la base de datos (emitidas por el banco, las aseguradoras y RELIANCE)
	X		Microsoft Excel	Asignación de la base de clientes a cada ejecutivo
		X		Gestión necesaria para contactar al cliente.
	X		SIBROK - Microsoft Excel	Validación de información del cliente
	X		Microsoft Excel	Cotización de póliza de entre las distintas aseguradoras asociadas.
	X		Microsoft Excel - Correo Electrónico - Impresora	Emisión de certificado de seguro en caso de haber acuerdo

ÁREA	ACTIVIDAD RELACIONADA CON TI		RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SI	NO		
		X		Envío de certificado firmado a la compañía de seguros
	X		SIBROK	Entrega de certificados a cobranzas para cobro
	X		SIBROK	Ingreso de facturas de listado de pagos de producción mensual
	X		SIBROK	Pago de primas acreditado a la cuenta de la compañía de seguros
	X		Microsoft Excel - Impresora	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro (listado de clientes generado en colaboración con Banco Promerica y RELIANCE)
Cobranzas		X		Recepción de pólizas
		X		Validación de la información de las pólizas
		X	Aprobar	Recepción de valores correspondientes a los pagos de la póliza
	X		Microsoft Excel - Impresora	Generar facturas
		X		Depósito de pagos de las pólizas
	X		SIBROK	Consolidación de cuentas
Siniestros		X		Recibir notificación del incidente por parte del cliente.
	X		Microsoft Excel - SIBROK	Registrar el incidente
	X		Correo Electrónico - Adobe Acrobat - Microsoft Office	Asesorar al cliente en los trámites necesarios para reportar a la aseguradora del incidente.
	X		Microsoft Excel	Dar seguimiento al incidente para garantizar la satisfacción del cliente

ÁREA	ACTIVIDAD RELACIONADA CON TI		RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SI	NO		
Dirección		X		Coordinar las tareas entre las áreas.
		X		Vigilar que se estén siguiendo las normas y procedimientos establecidos
	X		Microsoft Excel (Reporte Mensual)	Evaluar el desempeño del personal
		X		Realizar el mejoramiento continuo de los procesos.
		X		Dar atención de reclamos de clientes descontentos
	X		Microsoft Excel	Llevar un control interno de los ingresos y egresos
	X		Microsoft Word	Planificación de recursos humanos
	X		Microsoft Excel - Impresora	Elaborar rol de pagos
	X		Correo Electrónico	Aprobación de adquisición de insumos
Gerencia	X		Correo Electrónico- Microsoft Word - Adobe Acrobat - Impresora	Realizar negociaciones de los planes de seguros.
	X		Microsoft Excel - Impresora - Proyector	Presentación de informes de las actividades de la compañía a los socios
Asistencia Médica	X			Recepción de solicitudes de seguros médicos.
	X			Validación de la documentación proporcionada con la solicitud
	X		Microsoft Excel	Registro del asegurado
	X		Correo Electrónico - Microsoft Word - Adobe Acrobat	Envío de certificado firmado a la compañía de seguros
	X		Microsoft Excel	Emisión de facturas

ÁREA	ACTIVIDAD RELACIONADA CON TI		RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SI	NO		
	X		Microsoft Excel	Recepción de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.
		X		Validación de la información adjunta al reclamo
	X		Correo Electrónico - Microsoft Excel	Dar seguimiento del reclamo.
Recepción	X		Microsoft Excel	Control del Libro Diario
	X		Microsoft Excel	Control de Memorándumes emitidos
		X		Recepción de mensajería
		X		Recepción de llamadas

Tabla 3.1: Actividades del Negocio Relacionadas con TI

3.1.2. ACTIVIDADES CLAVES DEL NEGOCIO RELACIONADAS CON TI

En la Tabla 3.2 se representan las actividades claves del negocio y el servicio de TI con el que tienen relación.

ÁREA	RELACIÓN CON TI (Servicio)	ACTIVIDADES
Emisión	Microsoft Excel - Impresora	Emisión del certificado del seguro(5 copias)
	Correo Electrónico - fax	Envío de certificados a Ejecutivos de Banco Promerica
	Correo Electrónico - Adobe Acrobat	Envío de certificado firmado a la compañía de seguros
	Correo Electrónico - Adobe Acrobat	Pedido de facturación a la compañía de seguros

ÁREA	RELACIÓN CON TI (Servicio)	ACTIVIDADES
	SIBROK -Microsoft Excel	Verificación de datos del certificado versus Factura
	SIBROK	Ingreso de facturas de listado de pagos de producción mensual
	SIBROK	Pago de primas acreditado a la cuenta de la compañía de seguros
Renovación	SIBROK -Correo Electrónico - Microsoft Excel	Generación de la base de datos de clientes con pólizas a vencer
	SIBROK -Correo Electrónico - Microsoft Excel	Validación de la información de la base de datos (emitidas por el banco, las aseguradoras y RELIANCE)
	Microsoft Excel	Asignación de la base de clientes a cada ejecutivo
	SIBROK - Microsoft Excel	Validación de información del cliente
	Microsoft Excel	Cotización de póliza de entre las distintas aseguradoras asociadas.
	Microsoft Excel - Correo Electrónico -Impresora	Emisión de certificado de seguro en caso de haber acuerdo
	SIBROK	Entrega de certificados a cobranzas para cobro
	SIBROK	Ingreso de facturas de listado de pagos de producción mensual
	SIBROK	Pago de primas acreditado a la cuenta de la compañía de seguros
	Microsoft Excel - Impresora	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro (listado de clientes generado en colaboración con Banco Promerica y RELIANCE)
Cobranzas	Microsoft Excel - Impresora	Generación de facturas
	SIBROK	Consolidación de cuentas
Siniestros	Microsoft Excel - SIBROK	Registrar el incidente

ÁREA	RELACIÓN CON TI (Servicio)	ACTIVIDADES
	Correo Electrónico - Adobe Acrobat - Microsoft Office	Asesorar al cliente en los trámites necesarios para reportar a la aseguradora del incidente.
	Microsoft Excel	Dar seguimiento al incidente para garantizar la satisfacción del cliente
Dirección	Microsoft Excel (Reporte Mensual)	Evaluar el desempeño del personal
	Microsoft Excel	Llevar un control interno de los ingresos y egresos
	Microsoft Word	Planificación de recursos humanos
	Microsoft Excel - Impresora	Elaborar rol de pagos
	Correo Electrónico	Aprobación de adquisición de insumos
Gerencia	Correo Electrónico- Microsoft Word - Adobe Acrobat -Impresora	Realizar negociaciones de los planes de seguros.
	Microsoft Excel - Impresora - Proyector	Presentación de informes de las actividades de la compañía a los socios
Asistencia Médica como un Servicio por Relación con el Banco	Microsoft Excel	Registro del asegurado
	Correo Electrónico - Microsoft Word - Adobe Acrobat	Envío de certificado firmado a la compañía de seguros
	Microsoft Excel	Emisión de facturas
	Microsoft Excel	Recepción de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.
	Correo Electrónico - Microsoft Excel	Dar seguimiento del reclamo.
Recepción	Microsoft Excel	Control del Libro Diario
	Microsoft Excel	Control de Memorándumes emitidos

Tabla 3.2: Actividades Claves del Negocio Relacionadas con TI

3.2. ELEMENTOS DE CONFIGURACIÓN (CI)

“Los elementos de configuración son todos los componentes de la infraestructura tecnológica de la organización. Tales componentes son los que proveen los servicios de TI, para facilitar las actividades de la organización.

Los elementos de configuración incluyen hardware, software y la documentación necesaria que permite gestionar a la infraestructura tecnológica de la organización.”[22]

3.2.1. ELEMENTOS DE CONFIGURACIÓN DE HARDWARE

A continuación se presenta una lista de todos los dispositivos de hardware que forman parte de la infraestructura tecnológica de RELIANCE.

Los dispositivos de hardware considerados como elementos de configuración son los siguientes:

- Ordenadores (PCs)
- Impresoras
- Switch
- Modem
- Interfaces de Red
- Unidades de Almacenamiento
- Modem
- Alimentador de Energía Alterna (UPS)

[22] Osiatis. Gestión de la Disponibilidad. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_disponibilidad/proceso_gestion_de_la_disponibilidad/planificacion_de_la_disponibilidad.php. 25-06-2010

3.2.1.1. ORDENADORES

La Tabla 3.3 contiene una lista con las respectivas características de los ordenadores que son administrados por el departamento de TI de RELIANCE.

El identificador **PC** representa a un computador.

ID	Nombre PC	Tipo CPU	RAM	Sistema Operativo	Cuenta del Usuario	Nombre del Usuario
PC1	ACARPIO	Intel(R) Pentium(R) 4 CPU 3.20GHz	512	Windows XP Professional 5.1	acarpio	Alejandro Carpio
PC2	AROMERO	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1	aromero	Adriana Romero
PC3	CARROYO	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1	carroyo	Carlos Arroyo
PC4	DPENA	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1	dpena	Daniela Peña
PC5	RELIANCE-27BC77	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1	kcevallos	Karina Cevallos
PC6	RELIANCE-578C7C	Intel(R) Pentium(R) 4 CPU 2.80GHz	512	Windows XP Professional 5.1	vtrujillo	Victor Trujillo
PC7	SERVIDOR	Dual-Core AMD Opteron 2.80GHz	2047	Windows Server 2003 R2 5.2	Administrador	Administrador
PC8	USER	Intel(R) Core(TM)2 CPU 6400 2.13GHz	2048	Windows XP Professional 5.1	sgranda	Santiago Granda

ID	Nombre PC	Tipo CPU	RAM	Sistema Operativo	Cuenta del Usuario	Nombre del Usuario
PC9	VARROYO	Intel(R) Pentium(R) 4 CPU 2.80GHz	768	Windows XP Professional 5.1	varroyo	Verónica Arroyo
PC10	Valued-4328f30C	Intel(R) Pentium(R) 4 CPU 2.80GHz	769	Windows XP Professional 5.1	jtorres	Jorge Torres

Tabla 3.3: Ordenadores Administrados por el Departamento de TI

3.2.1.2. IMPRESORAS

La Tabla 3.4 contiene una lista de todas las impresoras que están conectadas a PCs individuales de RELIANCE. Las impresoras de esta lista están compartidas en la red para el uso del resto de PCs de la organización.

La Tabla 3.5 contiene las características de la impresora multifuncional de RELIANCE. Esta impresora está conectada a la red de RELIANCE con su propia dirección IP. Esta impresora sirve a todas las áreas de la organización.

El identificador **I** representa una impresora.

ID	Nombre	Tipo	ID-PC
I1	Epson LX-300+	Matricial	PC2
I2	Epson LX-300+	Matricial	PC4
I3	Epson LX-300+	Matricial	PC5
I4	HP LaserJet P1505	Laser	PC6

Tabla 3.4: Impresoras Matriciales y de Tinta en Red Administrada por el Departamento de TI

ID	Nombre	Tipo	Memoria Principal	Adaptador de red	Dirección IP
I5	KONICA MINOLTA	Multifuncional	192	Ethernet 10/100 Base-T	192.168.0.30

Tabla 3.5: Impresora Multifunción en Red Administrada por el Departamento de TI

3.2.1.3. SWITCH

En la Tabla 3.6 se presentan las respectivas características del único Switch que es administrado por el departamento de TI de RELIANCE.

El identificador **SWT** representa a un switch.

ID	Modelo	Numero de Puertos
SWT1	NETGEAR Switch Ethernet	24

Tabla 3.6: Switch Administrado por el Departamento de TI

3.2.1.4. MODEM

En la Tabla 3.7 se presentan las respectivas características del dispositivo de Modem que es administrado por el departamento de TI. Este modem permite tener conexión a la red de internet.

El identificador **M** representa a un modem.

ID	Nombre	Tipo
M1	TuchStone	TM602G

Tabla 3.7: Modem Administrado por el Departamento de TI

3.2.1.5. INTERFACES DE RED

En la Tabla 3.8 se presenta una lista de las interfaces de red que son administradas por el departamento de TI.

El identificador **NC** representa al dispositivo de una tarjeta de red, que permite a los PCs conectarse a la red de RELIANCE.
El identificador **MC** representa al dispositivo de modem, por medio del cual la organización tiene conexión a internet.

ID	Interfaz de Red	IP Dirección	Dominio	ID-PC
NC1	Broadcom NetXtreme Gigabit Ethernet	192.168.0.7	RELIANCE	PC1
NC2	Intel(R) PRO/100 VE Network Connection	192.168.0.3	RELIANCE	PC2
NC3	Intel(R) PRO/100 VE Network Connection	192.168.0.8	RELIANCE	PC3
NC4	Intel(R) PRO/100 VE Network Connection	192.168.0.9	RELIANCE	PC4
NC5	Intel(R) PRO/100 VE Network Connection	192.168.0.5	RELIANCE	PC5
NC6	Broadcom 440x 10/100 IntegratedController	192.168.0.4	RELIANCE	PC6
NC7	Adaptador PCI 10/100 AN 983 de ADMtek	10.10.10.10	RELIANCE	PC7
MC1	HP NC320i PCIe Gigabit Server Adapter	192.168.0.200		
NC8	Broadcom NetXtreme Gigabit Ethernet	192.168.0.15	RELIANCE	PC8
NC9	Intel(R) PRO/100 VE Network Connection	192.168.0.1	RELIANCE	PC9
NC10	Intel(R) PRO/100 VE Network Connection	192.168.0.6	RELIANCE	PC10

Tabla 3.8: Interfaces de Red Administradas por el Departamento de TI

3.2.1.6. UNIDADES DE ALMACENAMIENTO

En la Tabla 3.9 se presenta una lista de los tipos de unidades de almacenamiento que son administrados por el departamento de TI.

El identificador **HD** representa al dispositivo de disco duro.

El identificador **CD** representa al dispositivo de CD-ROM.

El identificador **DVD** representa al dispositivo de DVD-ROM.

ID	Nombre de la Unidad	Tipo de la Unidad	Tamaño	ID-PC
HD1	SAMSUNG HD080HJ/P	Unidad de disco	80GB	PC1
CD1	LITE-ON COMBO SHC-48S7K	Unidad de CD-ROM		
HD2	ST340014A	Unidad de disco	40GB	PC2
CD2	LITE-ON CD-ROM LTN-487T	Unidad de CD-ROM		
HD3	Maxtor 6E040L0	Unidad de disco	40GB	PC3
CD3	TSSTcorp CD-R/RW SH-R522C	Unidad de CD-ROM		
HD4	ST340014A	Unidad de disco	40GB	PC4
CD4	LITE-ON CD-ROM LTN-487T	Unidad de CD-ROM		
HD5	ST340014A	Unidad de disco	40GB	PC5
CD5	LITE-ON CD-ROM LTN-487T	Unidad de CD-ROM		
HD6	ST340015A	Unidad de disco	40GB	PC6
CD6	LITEON CD-ROM LTN486S	Unidad de CD-ROM		
HD7	FB160C4081	Unidad de disco	160GB	PC7
DVD1	HL-DT-ST RW/DVD GCC-H30N	Unidad de DVD-ROM		
HD8	SAMSUNG HD252HJ	Unidad de disco	250GB	PC8
CD7	HL-DT-ST DVDRAM GH20NS10	Unidad de CD-ROM		
HD9	MAXTOR STM3160215A	Unidad de disco	160GB	PC9
CD8	LITE-ON LTR-48327S	Unidad de CD-ROM		
CD9	HL-DT-ST DVD-RAM GSA-H58N	Unidad de CD-ROM		
HD10	ST340014A	Unidad de disco	80GB	PC10
CD10	LITE-ON CD-ROM LTN-487T	Unidad de CD-ROM		

Tabla 3.9: Unidades de Almacenamiento Administradas por el Departamento de TI

3.2.1.7. ALIMENTADOR DE ENERGÍA ALTERNA (UPS)

En la Tabla 3.10 se presenta el dispositivo de alimentación de energía alterna (UPS), que es administrado por el departamento de TI.
El identificador **UPS** representa al dispositivo de alimentación de energía alterna.

ID	Tipo
UPS1	UPS

Tabla 3.10: Alimentador de Energía Alterna Administrado por el Departamento de TI

3.2.2. ELEMENTOS DE CONFIGURACIÓN DE SOFTWARE

A continuación se presenta una lista de todo el software que es administrado por el departamento de TI de RELIANCE.

3.2.2.1. HERRAMIENTAS

En la Tabla 3.11 se presenta una lista general de las herramientas de software que son administradas por el departamento de TI.

El identificador **SW** representa a una herramienta de software.

ID	Software	Editor del Software
SW1	7-Zip	7-Zip
SW2	ABBYYFineReader 6.0 Sprint	ABBYY Software House
SW3	AcronisBackup Server	Acronis
SW4	Adobe Reader	Adobe Systems
SW5	Compresor WinRAR	WinRAR
SW6	CrystalReports	Seagate Software, Inc.
SW7	Logmein	Logmein
SW8	Microsoft Office Professional Edition 2003	Microsoft Corporation

SW9	MiraScan 6.2 (5000)	BenqScan
SW10	Mozilla Firefox	Mozilla
SW11	Nero 8	Nero AG
SW12	Outlook Express	Microsoft Corporation
SW13	Paquete de compatibilidad para 2007 Office system	Microsoft Corporation
SW14	PowerISO	PowerISO
SW15	SolidConverterPDF	SolidDocuments
SW16	Trend Micro Client/Server Security Agent	Trend Micro
SW17	WinZip	Winzip

Tabla 3.11: Aplicaciones de Software Administradas por el Departamento de TI

En la Tabla 3.12 se presenta una lista general de las aplicaciones de software, con su respectiva frecuencia de uso.

ID	Software	Frecuencia de Uso
SW4	Adobe Reader	Frecuente
SW7	Logmein	Frecuente
SW8	Microsoft Office Professional Edition 2003	Frecuente
SW12	Outlook Express	Frecuente
SW16	Trend Micro Client/Server Security Agent	Frecuente
SW1	7-Zip	Ocasional
SW2	ABBYYFineReader 6.0 Sprint	Ocasional
SW3	AcronisBackup Server	Ocasional
SW5	Compresor WinRAR	Ocasional
SW6	CrystalReports	Ocasional
SW9	MiraScan 6.2 (5000)	Ocasional
SW11	Nero 8	Ocasional
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional
SW14	PowerISO	Ocasional
SW15	SolidConverterPDF	Ocasional
SW17	WinZip	Ocasional
SW10	Mozilla Firefox	Rara vez

Tabla 3.12: Frecuencia de Uso de las Aplicaciones de Software Administradas por el Departamento de TI

La Tabla 3.13 contiene una lista de las aplicaciones de software, con su respetiva frecuencia de uso, distribuidas de acuerdo a cada PC que es administrado por el departamento de TI.

ID	Software	Frecuencia de Uso	ID-PC
SW2	ABBYYFineReader 6.0 Sprint	Ocasional	PC1
SW4	Adobe Reader	Frecuente	
SW5	Compresor WinRAR	Ocasional	
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW4	Adobe Reader	Frecuente	PC2
SW5	Compresor WinRAR	Ocasional	
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW4	Adobe Reader	Frecuente	PC3
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	
SW4	Adobe Reader	Frecuente	PC4
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	
SW4	Adobe Reader	Frecuente	PC5

ID	Software	Frecuencia de Uso	ID-PC
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	
SW5	Compresor WinRAR	Ocasional	PC6
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW1	7-Zip	Ocasional	PC7
SW4	Adobe Reader	Frecuente	
SW7	Logmein	Frecuente	
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW10	Mozilla Firefox	Rara vez	
SW11	Nero 8	Ocasional	
SW12	Outlook Express	Frecuente	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW1	7-Zip	Ocasional	PC8
SW2	ABBYYFineReader 6.0 Sprint	Ocasional	
SW3	AcronisBackup Server	Ocasional	
SW4	Adobe Reader	Frecuente	
SW5	Compresor WinRAR	Ocasional	
SW6	CrystalReports	Ocasional	
SW7	Logmein	Frecuente	
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW10	Mozilla Firefox	Rara vez	
SW11	Nero 8	Ocasional	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW14	PowerISO	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	

ID	Software	Frecuencia de Uso	ID-PC
SW4	Adobe Reader	Frecuente	PC9
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW10	Mozilla Firefox	Rara vez	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW15	SolidConverterPDF	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	
SW4	Adobe Reader	Frecuente	PC10
SW8	Microsoft Office Professional Edition 2003	Frecuente	
SW9	MiraScan 6.2 (5000)	Ocasional	
SW10	Mozilla Firefox	Rara vez	
SW12	Outlook Express	Frecuente	
SW13	Paquete de compatibilidad para 2007 Office system	Ocasional	
SW16	Trend Micro Client/Server Security Agent	Frecuente	
SW17	WinZip	Ocasional	

Tabla 3.13: Frecuencia de Uso por PC de las Herramientas de Software Administradas por el Departamento de TI

3.2.2.2. SISTEMAS DE GESTIÓN DE BRÓKERES DE SEGUROS

En la Tabla 3.14 se presenta una las características del sistema de gestión de brókeres de seguros, administrados por el departamento de TI.

El identificador **S** representa el sistema de gestión e brókeres de seguros.

ID	SISTEMA	PROPIETARIO
S1	SIBROK	RELIANCE

Tabla 3.14: Sistema de Gestión de Brókeres de Seguros Administrado por el Departamento de TI

3.2.2.3. SISTEMAS OPERATIVOS

En la Tabla 3.15 se presenta una lista de los sistemas operativos que son administradas por el departamento de TI.

El identificador **SO** representa al tipo de Sistema Operativo.

ID	Tipo
SO1	Windows XP Professional SP3
SO2	Windows Server 2003 R2

Tabla 3.15: Sistemas Operativos Administrados por el Departamento de TI

3.3. DETERMINACIÓN DE REQUISITOS DE DISPONIBILIDAD

3.3.1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

Para la obtención de los datos que se usan en la elaboración del Plan de Disponibilidad, se realizaron encuestas y entrevistas a los diferentes ejecutivos y personal que labora en RELIANCE. El formato de estas encuestas se encuentra en el Anexo 1: Formato para Funciones y Procesos del Negocio donde constan los siguientes datos: Nombre del proceso, objetivos, personal encargado del proceso, tecnologías de la información involucrada con el proceso, puntos de control, políticas, diagramas de flujo y la relación con otros procesos del negocio. Estos datos se utilizarán especialmente a lo largo del desarrollo del análisis de impacto.

3.3.1.1. OBJETIVOS Y ALCANCE

3.3.1.1.1. OBJETIVOS

- Identificar el impacto de una interrupción en el negocio.
- Definir los lineamientos para recuperar los procesos críticos del negocio una vez ocurrida la interrupción.

- Emitir información gerencial para la toma de decisiones sobre:
    - Áreas críticas del negocio
    - Impacto operacional de la interrupción del negocio.
    - Capacidades actuales de recuperación.
- Realizar estimaciones para el Plan de Disponibilidad, de acuerdo a los resultados obtenidos en el BIA.

3.3.1.1.2. ALCANCE

El presente análisis de impacto al negocio está dirigido en forma exclusiva al departamento de TI de RELIANCE. Este análisis permitirá determinar el impacto que provocará la caída de un servicio TI en las actividades del negocio, y las posibles medidas que se tomarán para recuperar los sistemas, recursos y datos, y así mantener la disponibilidad de los servicios de TI, teniendo en cuenta el soporte y el mantenimiento de los mismos.

3.3.1.2. IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DEL NEGOCIO

A continuación se identificará las funciones y procesos del negocio, donde las áreas de RELIANCE, son las siguientes:

- Emisión
- Renovación
- Cobranzas
- Siniestros
- Dirección
- Gerencia
- Asistencia médica
- TI (Sistemas)

En la Tabla 3.16 se detallan las funciones y procesos del negocio:

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO
Emisión	Recepción de Solicitudes de Póliza
	Emisión y envío de certificados de seguros
	Facturación a la compañía de seguros
	Pago de primas acreditado a la cuenta de la compañía de seguros
Renovación	Generación de la base de datos de clientes con pólizas a vencer
	Asignación de la base de clientes a cada ejecutivo
	Gestión para contactar al cliente.
	Cotización de póliza de entre las distintas aseguradoras asociadas.
	Emisión y envío de certificado de seguro en caso de haber acuerdo
	Ingreso de facturas de listado de pagos de producción mensual
	Pago de primas acreditado a la cuenta de la compañía de seguros
	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza
	Generación de facturas
	Depósito de pagos de las pólizas
	Consolidación de cuentas
Siniestros	Notificación y registro de incidentes
	Asesoría y seguimiento de incidentes
Dirección	Coordinar las tareas entre las áreas
	Evaluar el desempeño del personal
	Realizar el mejoramiento continuo de los procesos
	Atención de reclamos de clientes descontentos
	Control interno de los ingresos y egresos
	Planificación de recursos humanos
	Elaboración de rol de pagos
	Aprobación de adquisición de insumos
Gerencia	Negociaciones de los planes de seguros
	Presentación de informes de las actividades de la compañía a los socios
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.
	Registro del asegurado

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO
	Emisión de certificado de seguros
	Emisión de facturas
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.
Recepción	Control del Libro Diario
	Control de Memorándumes emitidos
TI (Sistemas)	Creación de Usuarios
	Obtención de Backups
	Mantenimiento de Comunicaciones
	Mantenimiento de Hardware
	Mantenimiento de Software
	Adquisición de Equipos
	Adquisición de Software
	Soporte a Usuarios
	Capacitación a Usuarios
	Mantenimiento y soporte del sistema SIBROK
	Manejo de Cableado y equipos electrónicos
	Elaboración de reportes de producción
	Ingreso de pólizas de seguro
	Renovación de seguros
	Depuración de la información

Tabla 3.16: Funciones y Procesos de RELIANCE

3.3.1.3. EVALUACIÓN DE IMPACTO FINANCIERO Y OPERACIONAL

En esta sección se evalúa el impacto financiero y operacional de los procesos en RELIANCE considerando si se presentase una interrupción de los procesos o un desastre. El impacto financiero será evaluado de forma cualitativa en todos los casos, esto se debe a que las cifras reales son consideradas como información confidencial para RELIANCE.

3.3.1.3.1. EVALUACIÓN DEL IMPACTO FINANCIERO

Para la Evaluación del Impacto Financiero se toma a consideración los siguientes valores:

0: no produce impacto = Ponderación ***0-5***
1: bajo impacto = Ponderación **6-10**
2: impacto medio = Ponderación **11-15**
3: alto impacto = Ponderación **16 – 25**

La Tabla 3.17 se observar la valoración de cada una de los factores en los procesos, el impacto financiero final es resultado de una equivalencia de la ponderación.

3.3.1.3.2. EVALUACIÓN DEL IMPACTO OPERACIONAL

A continuación en la Tabla 3.18 se representa la evaluación del impacto operacional en RELIANCE, para lo cual se han tomado como factores representativos en esta evaluación:

- Flujo de caja
- Satisfacción del cliente
- Posicionamiento en el mercado

Para medir esta evaluación se han tomado los siguientes valores:
0: no produce impacto = ***Ninguno***
1: bajo impacto = ***Bajo***
2: impacto medio = ***Medio***
3: alto impacto = ***Alto***

El análisis de impacto operacional del factor de Flujo de Caja posee un valor alto de impacto, debido a que el movimiento financiero dentro de la organización es de suma importancia para la observación y análisis de las entradas y salidas de dinero que permiten la ejecución de las actividades de la empresa.

Renovación	distintas aseguradoras asociadas.	1	1	0	2	0	0	1	0	1	2	8	1	La mayoría de clientes continúan con la misma aseguradora son muy pocos quienes piden cotizaciones para elegir
	Emisión y envío de certificado de seguro en caso de haber acuerdo	3	3	2	3	0	0	2	0	1	2	16	3	Debido a que la póliza no es registrada en la aseguradora correspondiente, se puede perder la confianza del cliente
	Ingreso de facturas de listado de pagos de producción mensual	1	2	2	3	0	0	2	0	1	2	13	2	De no realizarse las facturas no se realiza un desembolso a las aseguradoras y no son mostradas en el reporte de producción mensual
	Pago de primas acreditado a la cuenta de la compañía de seguros	2	2	1	2	0	0	2	2	1	2	14	2	De no realizarse el pago a tiempo o en el plazo establecido se puede perder a un socio/aliado que brinda servicios a la compañía
	Generación y envió de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro	2	2	0	3	0	0	2	0	1	2	12	1	De no ser enviados la compañía puede verse a afrontar requisitos legales y regulatorios entre RELIANCE Y BANCO PROMERICA
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza	3	3	3	3	0	0	2	0	1	2	17	3	De no ser darse la compañía no tendría ingresos y estaría retrasado en el pago de sus haberes
	Genera ración de facturas	3	3	2	2	0	0	2	0	1	2	15	2	De no realizarse las facturas no se realiza un desembolso a las aseguradoras y no son mostradas en el reporte de producción mensual
	Depósito de pagos de las pólizas	3	3	0	2	0	0	3	0	1	2	14	2	Los pagos son ingresados en una sola cuenta para posteriormente realizar la cancelación de facturas y nomina
	Consolidación de cuentas	3	3	2	3	0	0	3	0	1	2	17	3	Debe ser realizado para tener presente que pólizas son canceladas para conocer a que aseguradora debe ser entregado
Siniestros	Notificación y registro de incidentes	0	0	1	3	0	0	2	0	1	2	9	1	De darse un siniestro el cliente está en su derecho de notificarlo y es registrado como historial de riesgo
	Asesoría y seguimiento de incidente	0	0	0	3	0	0	3	0	1	2	9	1	Garantizar la satisfacción del cliente.
Dirección	Coordinar las tareas entre las áreas	1	0	0	1	0	0	1	0	1	1	5	0	Las funciones están claramente definidas por lo que no es necesario que este constantemente detrás de ellas
	Evaluar el desempeño del personal	0	0	0	1	0	0	1	0	1	1	4	0	Se lo realiza de forma periódica
	Realizar el mejoramiento continuo de los procesos	0	1	0	1	0	0	1	0	1	1	5	0	Se considera que los procesos están lo suficiente maduros como para sufrir cambios constantes
	Atención de reclamos de clientes descontentos	2	2	1	1	0	0	3	2	2	1	14	2	Lo más importante es tener al cliente satisfecho por el servicio y trato brindado de no ser así se pierde al cliente y sus recomendados
	Control interno de los ingresos y egresos	3	2	3	3	3	0	2	2	2	3	23	3	Se encarga de dar un seguimiento a la cartera del negocio
	Planificación de recursos humanos	0	0	0	1	0	0	1	0	1	1	4	0	Debe haber una correcta planificación para que no afecte la producción en caso de ausencia de personal.
	Elaboración de rol de pagos	2	0	0	1	0	0	1	0	1	3	8	1	De no darse en el plazo establecido por la ley la empresa está sujeta a requisitos legales y regulatorios
	Aprobación de adquisición de insumos	2	2	1	2	2	0	1	0	1	2	13	2	Se realiza un desembolso de dinero al adquirir un producto necesario
Gerencia	Negociaciones de los planes de seguros	3	3	0	2	0	0	1	0	1	1	11	2	Se requiere de nuevos y mejores servicios y productos para poder ser más competitivos
	Presentación de informes de las actividades de la compañía a los socios	0	0	2	1	0	0	1	0	1	1	6	1	Se debe presentar un informe de estado de la compañía
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.	3	3	3	3	0	0	2	0	1	2	17	3	Debido a que si no se reciben nuevas pólizas no se tienen nuevos clientes y los ingresos en la compañía disminuyen
	Registro del asegurado	2	0	2	2	0	0	1	0	1	2	10	1	Debe realizarse la apertura del historial del cliente
	Emisión de certificado de seguros	1	2	2	3	0	0	2	0	1	2	13	2	Debido a que la póliza no es registrada en la aseguradora correspondiente, se puede perder la confianza del cliente
	Emisión de facturas	2	2	2	2	0	0	2	0	1	2	13	2	De no realizarse las facturas no se realiza un desembolso a las aseguradoras o emitidos los reembolsos a los asegurados adicionalmente no son mostradas en el reporte de producción mensual
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.	1	1	2	2	1	0	3	1	1	2	14	2	Se debe garantizar la satisfacción del cliente
Recepción	Control de libro diario	1	1	3	3	2	0	3	3	3	2	21	3	Debido a que si no se no se lleva un correcto control del mismo se tiene un desequilibrio en las finanzas y la imagen de la compañía se ve afectada.
	Control de Memorándumes	1	1	3	3	2	0	2	2	2	2	18	3	Debido a que con ellos se realiza las comunicaciones a clientes y aseguradoras y deben ser consecutivos.
	Creación de Usuarios	0	0	0	1	0	0	1	0	1	2	5	0	No interrumpe las labores del usuario si este no es ingresado en el Active Directory
	Obtención de Backups	2	2	3	3	3	0	2	2	2	3	22	3	Los respaldos de la información son muy importantes frente a una recuperación de servicios.
	Mantenimiento de Comunicaciones	2	3	2	3	3	0	1	0	1	3	18	3	A través de la red se provee muchos de los servicios que brinda TI para las funciones diarias de los usuarios.
	Mantenimiento de Hardware	2	2	2	3	3	0	1	0	1	2	16	3	Se puede perder activos de la compañía entre estos la información.
														Si no se da un correcto mantenimiento del software si uno

Al factor de Satisfacción del Cliente se le asignado un valor medio de impacto debido a que el flujo de dinero es independiente de la satisfacción del cliente, pero se toma en cuenta la relación que existe entre ambos factores como por ejemplo en la cotización y pago de las pólizas.

El factor de Posicionamiento en el Mercado posee un valor medio de impacto, debido a que si se da una interrupción de los servicios de TI, este impacto afectara a la difusión y promoción de los servicios que ofrece la organización, como por ejemplo en la atención de reclamos de clientes descontentos, y los procesos necesarios para la atención de los mismos. Si un cliente se encuentra insatisfecho por el servicio prestado dejará a la organización y esto implica ya una pérdida para el negocio y con esto se reduce el nivel de posicionamiento en el mercado de la organización.

FUNCIÓN DEL NEGOCIO	**PROCESO DEL NEGOCIO**	**CLASIFICACIÓN DEL IMPACTO OPERACIONAL**		
		Flujo de Caja	**Satisfacción del Cliente**	**Posicionamiento en el Mercado**
Emisión	Recepción de Solicitudes de Póliza	0	3	2
	Emisión y envío de certificados de seguros	0	1	2
	Facturación a la compañía de seguros	3	1	1
	Pago de primas acreditado a la cuenta de la compañía de seguros	3	1	2
Renovación	Generación de la base de datos de clientes con pólizas a vencer	0	0	0

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL		
		Flujo de Caja	Satisfacción del Cliente	Posicionamiento en el Mercado
	Asignación de la base de clientes a cada ejecutivo	2	0	0
	Gestión para contactar al cliente	0	3	2
	Cotización de póliza de entre las distintas aseguradoras asociadas	3	2	2
	Emisión y envío de certificado de seguro en caso de haber acuerdo	0	1	1
	Ingreso de facturas de listado de pagos de producción mensual	3	0	0
	Pago de primas acreditado a la cuenta de la compañía de seguros	3	1	2
	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro	1	2	2
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza	3	2	0
	Generación de facturas	3	1	2
	Depósito de pagos de las pólizas	3	2	2

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL		
		Flujo de Caja	Satisfacción del Cliente	Posicionamiento en el Mercado
	Consolidación de cuentas	3	0	1
Siniestros	Notificación y registro de incidentes	1	3	2
	Asesoría y seguimiento de incidente	0	3	2
Dirección	Coordinar las tareas entre las áreas	0	0	0
	Evaluar el desempeño del personal	0	1	0
	Realizar el mejoramiento continuo de los procesos	0	0	2
	Atención de reclamos de clientes descontentos	0	3	1
	Control interno de los ingresos y egresos	3	0	0
	Planificación de recursos humanos	0	0	1
	Elaboración de rol de pagos	3	0	0
	Aprobación de adquisición de insumos	2	0	0
Gerencia	Negociaciones de los planes de seguros	0	0	3
	Presentación de informes de las actividades de la compañía a los socios	0	0	1

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL		
		Flujo de Caja	Satisfacción del Cliente	Posicionamiento en el Mercado
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.	0	2	1
	Registro del asegurado	0	1	0
	Emisión de certificado de seguros	0	1	1
	Emisión de facturas	3	1	2
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.	0	2	2
Recepción	Control del Libro Diario	0	0	1
	Control de Memorándumes emitidos	0	0	1
TI (Sistemas)	Creación de Usuarios	0	0	0
	Obtención de Backups	0	0	0
	Mantenimiento de Comunicaciones	0	3	3
	Mantenimiento de Hardware	0	0	0
	Mantenimiento de Software	0	0	0
	Adquisición de Equipos	0	0	0
	Adquisición de Software	0	0	0
	Soporte a Usuarios	0	2	0
	Capacitación a Usuarios	0	1	0

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL		
		Flujo de Caja	Satisfacción del Cliente	Posicionamiento en el Mercado
	Mantenimiento y soporte del sistema SIBROK	0	3	0
	Manejo de Cableado y equipos electrónicos	0	2	0
	Elaboración de reportes de producción	3	0	0
	Ingreso de pólizas de seguro	3	1	0
	Renovación de seguros	3	1	2
	Depuración de la información	0	0	0

Tabla 3.18: Evaluación del Impacto Operacional[24]

3.3.1.4. IDENTIFICACIÓN DE PROCESOS CRÍTICOS DEL NEGOCIO

Con los resultados obtenidos del Impacto Financiero y del Impacto Operacional por medio de la Tabla 3.17 y la Tabla 3.18 respectivamente, se procede a la identificación de los procesos críticos del negocio.

A continuación en la Tabla 3.19 se presenta la suma de los valores obtenidos del análisis de impacto financiero y operacional, para obtener un valor total. Este total permitirá evaluar el tiempo máximo que un proceso puede estar fuera de servicio.

[24] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
Emisión	Recepción de Solicitudes de Póliza	3	0	3	2	8
	Emisión y envío de certificados de seguros	2	0	1	2	5
	Facturación a la compañía de seguros	2	3	1	1	7
	Pago de primas acreditado a la cuenta de la compañía de seguros	2	3	1	2	8
Renovación	Generación de la base de datos de clientes con pólizas a vencer	2	0	0	0	2
	Asignación de la base de clientes a cada ejecutivo	1	2	0	0	3
	Gestión para contactar al cliente	2	0	3	2	7
	Cotización de póliza de entre las distintas aseguradoras asociadas	2	3	2	2	9
	Emisión y envío de certificado de seguro en caso de haber acuerdo	3	0	1	1	5
	Ingreso de facturas de listado de pagos de producción mensual	2	3	0	0	5

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Pago de primas acreditado a la cuenta de la compañía de seguros	2	3	1	2	8
	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro	2	1	2	2	7
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza	3	3	2	0	8
	Generación de facturas	2	3	1	2	8
	Depósito de pagos de las pólizas	2	3	2	2	9
	Consolidación de cuentas	3	3	0	1	7
Siniestros	Notificación y registro de incidentes	1	1	3	2	7
	Asesoría y seguimiento de incidente	1	0	3	2	6
Dirección	Coordinar las tareas entre las áreas	0	0	0	0	0
	Evaluar el desempeño del personal	0	0	1	0	1

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Realizar el mejoramiento continuo de los procesos	0	0	0	2	2
	Atención de reclamos de clientes descontentos	2	0	3	1	6
	Control interno de los ingresos y egresos	3	3	0	0	6
	Planificación de recursos humanos	0	0	0	1	1
	Elaboración de rol de pagos	1	3	0	0	4
	Aprobación de adquisición de insumos	2	2	0	0	4
Gerencia	Negociaciones de los planes de seguros	2	0	0	3	5
	Presentación de informes de las actividades de la compañía a los socios	1	0	0	1	2
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.	3	0	2	1	6
	Registro del asegurado	1	0	1	0	2
	Emisión de certificado de seguros	2	0	1	1	4
	Emisión de facturas	2	3	1	2	8

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.	2	0	2	2	6
Recepción	Control del Libro Diario	3	0	0	1	4
	Control de Memorándumes emitidos	3	0	0	1	4
TI (Sistemas)	Creación de Usuarios	0	0	0	0	0
	Obtención de Backups	3	0	0	0	3
	Mantenimiento de Comunicaciones	3	0	3	3	9
	Mantenimiento de Hardware	2	0	0	0	2
	Mantenimiento de Software	1	0	0	0	1
	Adquisición de Equipos	1	0	0	0	1
	Adquisición de Software	1	0	0	0	1
	Soporte a Usuarios	1	0	2	0	3
	Capacitación a Usuarios	1	0	1	0	2
	Mantenimiento y soporte del sistema SIBROK	3	0	3	0	6
	Manejo de Cableado y equipos electrónicos	1	0	2	0	3

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Elaboración de reportes de producción	3	3	0	0	6
	Ingreso de pólizas de seguro	3	3	1	0	7
	Renovación de seguros	3	3	1	2	9
	Depuración de la información	3	0	0	0	3

Tabla 3.19: Procesos Críticos del Negocio[25]

En la Tabla 3.19 se puede observar, que de los resultados obtenidos en la columna de Total, se pueden determinar qué procesos son considerados para el negocio como críticos. Por ejemplo el proceso de Recepción de Pólizas de Seguro posee un valor total de 8, el cual está en un rango superior a los demás valores del área de Emisiones y por tanto es considerado como el proceso más crítico de esta área, a diferencia del proceso de Emisión y Envío de Certificados de Seguros, el cual posee un valor total de 5, y por tanto es el proceso menos crítico de esta área. Esta diferencia de criticidad de procesos radica en que el proceso de Recepción de Pólizas de Seguro tiene como prioridad acoger pólizas de seguros de los clientes, lo que representa ganancia económica para la organización y por tanto, mayor impacto económico, así como la satisfacción el cliente y un mayor posicionamiento en el mercado. Por otro lado, el proceso de Emisión y Envío de Certificados de Seguros posee menos escala de criticidad que el proceso anterior, debido a que este proceso representa actividades de papeleo, y por tanto influye en tener un menor impacto financiero que el proceso descrito anteriormente, así como también posee menor prioridad en la satisfacción del cliente y en el posicionamiento del mercado.

[25] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

3.3.1.5. IDENTIFICACIÓN DE SISTEMAS Y APLICACIONES CRÍTICAS DE TI POR PROCESO DEL NEGOCIO

En la Tabla 3.20 se detallan los sistemas y aplicaciones críticas de TI por proceso del negocio. La Tabla 3.20 es un extracto de la tabla mostrada en el Anexo 2: Sistemas, Aplicaciones y Recursos Críticos de TI.

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE TI	
Emisión	Recepción de Solicitudes de Póliza	Microsoft Office	· Word
			· Excel
		Outlook Express	
		Scanner	
		Impresora	
		Fotocopiadora	
		Correo Electrónico	
		Adobe Reader	
	Emisión y envío de certificados de seguros	Microsoft Office	· Word
			· Excel
		Outlook Express	
		Scanner	
		Impresora	
		Fotocopiadora	
		Fax	
		Correo Electrónico	
		Adobe Reader	
	Facturación a la compañía de seguros	Microsoft Office	· Word
			· Excel
		Outlook Express	
		Scanner	
		Impresora	
		Fotocopiadora	
		Fax	
		SIBROK	· Formularios
			· Reportes
			· Consultas
		Intranet	
		Correo Electrónico	

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE TI	
	Pago de primas acreditado a la cuenta de la compañía de seguros	Microsoft Office	· Word
			· Excel
			· Power Point
		Scanner	
		Impresora	
		Fotocopiadora	
		Fax	
		SIBROK	· Formularios
			· Reportes
			· Consultas

Tabla 3.20: Sistemas y Aplicaciones Críticas de TI por Proceso del Negocio[26]

3.3.1.6. IDENTIFICACIÓN DE TIEMPOS MÁXIMOS DE CAÍDA (MTD)

Para identificar a los MTD's, se procede a utilizar el total de puntos obtenidos de la suma resultante entre el Impacto Financiero y el Impacto Operacional, estos resultados los obtenemos de la Tabla 3.19.

A continuación se define la escala de tiempos que se utilizará para identificar los valores de MTD a cada proceso del negocio:

A = De 1 a 24 horas

B = De 25 a 48 horas

C = De 49 a 72 horas

D = De 73 horas a 5 días

E = De 6 a 15 días

F = De 16 a 30 días

En la Tabla 3.21 se representan la escala de equivalencia para la definición de los MTD's, de acuerdo al total de puntos obtenidos en la Tabla 3.19.

[26] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

TOTAL Impacto Financiero + Impacto Operacional	MTD
9	A
8	A
7	A
6	B
5	B
4	C
3	C
2	D
1	E
0	F

Tabla 3.21: Escala de Equivalencia de MTD

A continuación en la Tabla 3.22 se representan los tiempos máximos de caída por cada proceso del negocio, donde el valor de MTD corresponde a la escala de equivalencia de la Tabla 3.21.

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	MTD
Emisión	Recepción de Solicitudes de Póliza	A
	Emisión y envío de certificados de seguros	B
	Facturación a la compañía de seguros	A
	Pago de primas acreditado a la cuenta de la compañía de seguros	A
Renovación	Generación de la base de datos de clientes con pólizas a vencer	D
	Asignación de la base de clientes a cada ejecutivo	C
	Gestión para contactar al cliente	A
	Cotización de póliza de entre las distintas aseguradoras asociadas	A
	Emisión y envío de certificado de seguro en caso de haber acuerdo	B
	Ingreso de facturas de listado de pagos de producción mensual	B
	Pago de primas acreditado a la cuenta de la compañía de seguros	A

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	MTD
	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro	A
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza	A
	Generación de facturas	A
	Depósito de pagos de las pólizas	A
	Consolidación de cuentas	A
Siniestros	Notificación y registro de incidentes	A
	Asesoría y seguimiento de incidente	B
Dirección	Coordinar las tareas entre las áreas	F
	Evaluar el desempeño del personal	E
	Realizar el mejoramiento continuo de los procesos	D
	Atención de reclamos de clientes descontentos	B
	Control interno de los ingresos y egresos	B
	Planificación de recursos humanos	E
	Elaboración de rol de pagos	C
	Aprobación de adquisición de insumos	C
Gerencia	Negociaciones de los planes de seguros	B
	Presentación de informes de las actividades de la compañía a los socios	D
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.	B
	Registro del asegurado	D
	Emisión de certificado de seguros	C
	Emisión de facturas	A
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.	B
Recepción	Control del Libro Diario	C
	Control de Memorándumes emitidos	C
TI (Sistemas)	Creación de Usuarios	F
	Obtención de Backups	C
	Mantenimiento de Comunicaciones	A
	Mantenimiento de Hardware	D
	Mantenimiento de Software	E
	Adquisición de Equipos	E
	Adquisición de Software	E
	Soporte a Usuarios	C
	Capacitación a Usuarios	E
	Mantenimiento y soporte del sistema SIBROK	B
	Manejo de Cableado y equipos electrónicos	C

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	MTD
	Elaboración de reportes de producción	B
	Ingreso de pólizas de seguro	A
	Renovación de seguros	A
	Depuración de la información	C

Tabla 3.22: Definición de MTD[27]

A continuación en la Tabla 3.23 y de acuerdo a los valores obtenidos en la Tabla 3.22, se representa el total de valores de MTD's que posee el negocio:

MTD	TOTAL
A	16
B	11
C	10
D	5
E	6
F	2

Tabla 3.23: Total de Valores de MTD's del Negocio

Como se puede observar los resultados obtenidos en la Tabla 3.22 y en la Tabla 3.23, verificamos que el negocio tiene un mayor número de procesos con valores de MTD's de A. Esta referencia indica que los procesos ubicados en esta escala, no pueden permanecer inactivos por más de 24 horas, ya que esto representaría para el negocio la pérdida de ganancias y acumulación de tareas para los empleados. Tal es el caso del proceso de Pago de Primas, correspondiente al área de Emisión, en donde si se da la caída de servicios de TI, no se podrán emitir el pago a la solicitudes de las pólizas de seguro de los clientes, lo que involucra un mayor impacto financiero para el negocio, así como también afecta a la satisfacción del cliente, el cual muestra su descontento por el servicio obtenido

[27] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

por parte del negocio, y esta insatisfacción del cliente también afecta al posicionamiento en el mercado del negocio.

También existen procesos con valores de MTD's de D, E y F; los cuales por poseer un mayor rango de tiempo de caída, no significa que sean ignorados o relegados a un segundo plano, por otra parte, también se los considera significativos, como por ejemplo el proceso de la Evaluación del Desempeño del Personal correspondiente al área de Dirección, donde este proceso posee un valor MTD de E, este proceso tiene su validez en determinar qué factores están afectando o cuáles podrían mejorar el desempeño del personal.

3.3.1.7. IDENTIFICACIÓN DEL TIEMPO OBJETIVO DE RECUPERACIÓN (RTO) Y DEL TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT)

3.3.1.7.1. TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)

A continuación se detalla la escala de tiempos que se requerirá para realizar la recuperación de un servicio que está fuera de operación:

A = De 1 a 24 horas
B = De 25 a 48 horas
C = De 49 a 72 horas
D = De 73 horas a 5 días
E = De 6 a 15 días
F = De 16 a 30 días
G = De 31 a 60 días

3.3.1.7.2. TIEMPO DE RECUPERACIÓN DE TRABAJO (WRT)

Entre los tiempos de recuperación de trabajo a ser considerados si el sistema SIBROK dejó de funcionar por un cierto periodo prolongado de tiempo, en este periodo no se podrá registrar a los nuevos clientes, los cuales requieren la

emisión de las pólizas de seguro; entonces este procedimiento se lo realizará por medio de herramientas alternas, hasta que el sistema sea restablecido. Una vez que el sistema vuelva a estar en operación, se procederá a registrar a los nuevos clientes que han sido habilitados mientras el sistema estaba fuera de servicio, este tiempo requerido para registrar a los clientes en el sistema, es el tiempo de recuperación de trabajo.

3.3.1.7.3. EVALUACIÓN DE RTO Y WRT

Para la evaluación de los tiempos de RTO en RELIANCE, primero se toma en cuenta la recuperación de los sistemas y recursos críticos de área de TI, debido a que son considerados como actividades bases, las cuales permiten poner en marcha las demás actividades del negocio. La escala para el RTO se la determina en función del tiempo, tal como se lo indica en la Tabla 3.24:

ACTIVIDAD DE TI	RTO (Horas)
Recuperación del sistema SIBROK	12
Recuperación del servidor de base de datos del sistema	24
Recuperación del servidor de correo electrónico	12
Recuperación de la red interna (LAN)	24
Recuperación de la intranet	24
Recuperación del enlace de red externo (Internet)	12
Recuperación del servicio de Active Directory	24

Tabla 3.24: Tiempo Objetivo de Recuperación (RTO) de las Actividades de TI

A continuación se representan los valores de RTO y WRT, para los procesos y servicios de TI, los cuales han sido definidos previamente en la Tabla 3.20. Los valores de RTO y WRT están representados en la Tabla 3.25, esta tabla es un extracto de la tabla del Anexo 3: Tiempos de Recuperación RTO y WRT por Procesos del Negocio.

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE TI		RTO (HORAS)	WRT (HORAS)
Emisión	Recepción de Solicitudes de Póliza	Microsoft Office	Word	2	1
			Excel	2	1
		Outlook Express		3	2
		Scanner		1	-
		Impresora		1	-
		Fotocopiadora		1	-
		Correo Electrónico		3	3
		Adobe Reader		2	2
	Emisión y envío de certificados de seguros	Microsoft Office	Word	2	1
			Excel	2	1
		Outlook Express		3	2
		Scanner		1	-
		Impresora		1	-
		Fotocopiadora		1	-
		Fax		1	-
		Correo Electrónico		3	3
		Adobe Reader		2	2
	Facturación a la compañía de seguros	Microsoft Office	Word	2	1
			Excel	2	1
		Outlook Express		3	2
		Scanner		1	-
		Impresora		1	-
		Fotocopiadora		1	-
		Fax		1	-
		SIBROK	Formularios	2	2
			Reportes	2	2
			Consultas	2	2
		Intranet		1	-
		Correo Electrónico		3	3
	Pago de primas acreditado a la cuenta de la compañía de seguros	Microsoft Office	Word	2	1
			Excel	2	1
			Power Point	2	1
		Scanner		1	-
		Impresora		1	-
		Fotocopiadora		1	-
		Fax		1	-
		SIBROK	Formularios	2	2
			Reportes	2	2
			Consultas	2	2

Tabla 3.25: RTO y WRT por Procesos del Negocio[28]

[28] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Como se puede observar en la Tabla 3.25, se han definido los tiempos de recuperación RTO y WRT para cada proceso del negocio. Por ejemplo, en el proceso de Facturación del área de Emisión se utiliza la aplicación del SIBROK, la cual tiene un valor de RTO de 2 horas, lo que nos indica que es el tiempo máximo de recuperación de la aplicación SIBROK, cuando está fuera de servicio, teniendo en cuenta que este valor es sólo para este proceso. De igual manera el proceso mencionado anteriormente, posee un valor de WRT de 2 horas, es decir que cuando la aplicación SIBROK ya esté en operación, luego de haber estado fuera de servicio, se tendrá un periodo de tiempo de 2 horas para restablecer toda la información que se ha generado durante el periodo de tiempo en que la aplicación estuvo fuera de servicio, teniendo en cuenta que esta información fue generada y respaldada por medio de otras herramientas, que en este caso para este proceso, se utilizan las hojas electrónicas de Excel.

3.3.1.8. IDENTIFICACIÓN DEL OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO)

A continuación se define el RPO para cada proceso del negocio, y de acuerdo a los sistemas y aplicaciones que utiliza cada proceso para cumplir con sus actividades. Los valores del RPO esta representados en la Tabla 3.26, esta tabla es un extracto del Anexo 4: Objetivo de Punto de Recuperación (RPO) por Procesos del Negocio.

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE TI		RPO
Emisión	Recepción de Solicitudes de Póliza	Microsoft Office	Word	<= 30 min
			Excel	<= 30 min
		Outlook Express		30 - 60 min
		Scanner		-
		Impresora		-
		Fotocopiadora		-
		Correo Electrónico		30 - 60 min

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE TI		RPO
		Adobe Reader		<= 30 min
	Emisión y envío de certificados de seguros	Microsoft Office	Word	<= 30 min
			Excel	<= 30 min
		Outlook Express		30 - 60 min
		Scanner		-
		Impresora		-
		Fotocopiadora		-
		Fax		-
		Correo Electrónico		30 - 60 min
		Adobe Reader		<= 30 min
	Facturación a la compañía de seguros	Microsoft Office	Word	<= 30 min
			Excel	<= 30 min
		Outlook Express		30 - 60 min
		Scanner		-
		Impresora		-
		Fotocopiadora		-
		Fax		-
		SIBROK	Formularios	<= 30 min
			Reportes	<= 30 min
			Consultas	<= 30 min
		Intranet		-
		Correo Electrónico		30 - 60 min
	Pago de primas acreditado a la cuenta de la compañía de seguros	Microsoft Office	Word	<= 30 min
			Excel	<= 30 min
			Power Point	<= 30 min
		Scanner		-
		Impresora		-
		Fotocopiadora		-
		Fax		-
		SIBROK	Formularios	<= 30 min
			Reportes	<= 30 min
			Consultas	<= 30 min

Tabla 3.26: Objetivo de Punto de Recuperación (RPO) por Procesos del Negocio[29]

[29] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Como se puede observar los resultados obtenidos en la Tabla 3.26, la organización tiene como valores de RPO un rango entre 30 a 60 minutos, que soportaría en la pérdida de datos y en términos de un período de tiempo que puede ser tolerado por un proceso del negocio. Tal es el caso del proceso de Facturación en el área de Emisión, si la aplicación SIBROK está fuera de servicio por un periodo prolongado de tiempo, este periodo no deberá sobrepasar los 30 minutos, debido que si esto sucede, no se podrán registrar los datos de los asegurados para la emisión de las nuevas pólizas, teniendo en cuenta que la aplicación es la que contiene los formularios necesarios para el registro de los nuevos clientes, así como también facilita las consultas sobre los datos de los clientes ya asegurados, lo que permite obtener reportes con la información de los clientes.

3.3.1.9. ANÁLISIS DEL DAÑO A CONSECUENCIA DE LA INTERRUPCIÓN DE UN SERVICIO DE TI

A continuación se procede a determinar las consecuencias que se darían a causa de la interrupción de un servicio o recurso de TI. Los datos de este análisis se encuentran representados en la Tabla 3.27.

SERVICIO DE TI	CONSECUENCIA
Microsoft Office Word	No permite el procesamiento de texto, para la elaboración de memos, cartas, solicitudes, certificados, etc.
Microsoft Office Excel	Impide y retrasa la elaboración reportes, para el procesamiento de textos y plantillas de cálculo en hojas electrónicas, para todas las áreas del negocio, desde la recepción de solicitudes de póliza hasta la emisión de las mismas.
Microsoft Office Power Point	No permite la elaboración de presentaciones gráficas, tal la realización de informativos, con respecto a la evaluación del desempeño del personal.
Outlook Express	Impide la descarga, el envío y la visualización de correos electrónicos, dentro y fuera de la organización. Tal como es el caso del envío de las pólizas de seguro a las compañías aseguradoras.

SERVICIO DE TI	CONSECUENCIA
Internet	No permite tener acceso a la red pública (internet), lo que impide tener conexión con otras redes, así como también no permite la transferencia de la información, tal como es el caso del envío de correos electrónicos fuera de la organización.
Scanner	La interrupción de este servicio impide la digitalización, captura de imágenes y documentos de texto, lo que provoca el retraso en la transferencia de la información, tal como es el caso del envío y emisión de las solicitudes de pólizas.
Impresora	No permite tener información impresa en papel de documentos, tales como la emisión de las pólizas de seguro. También provoca que no se pueda archivar las diferentes pólizas de seguro emitidas durante el día.
Fotocopiadora	Impide tener copias de los documentos que han sido generados durante el día laboral, como por ejemplo no se tendría copias de las facturas generadas.
Fax	No permite la transmisión y recepción de documentos mediante la red telefónica, como por ejemplo el envío de emisiones de pólizas de seguro.
UPS	Provoca la pérdida de información generada durante la jornada laboral y que no ha sido respaldada con anticipación.
SIBROK (Sistema Integrado de Brokers)	La interrupción de este servicio, impide a las áreas tener acceso a los formularios del sistema, así como la generación de reportes y la realización de consultas, con respecto a los clientes que poseen un seguro.
Intranet	La interrupción de este servicio impide a los usuarios no utilizar y visualizar la información publicada en la red interna del negocio.
Correo Electrónico	No permite a los usuarios enviar y recibir mensajes electrónicos, así como también enviar y recibir archivos, como por ejemplo el envío de copias en las emisiones de pólizas de seguro.
Servidor de Archivos	No permite a los usuarios tener acceso remoto y utilización de los archivos almacenados en el servidor.
Antivirus	Aumenta el riesgo de tener virus informáticos en las computadoras, lo que provoca el mal funcionamiento de las computadoras
Adobe Reader	Impide abrir, guardar, imprimir y compartir documentos electrónicos, que han sido creados con esta aplicación.

SERVICIO DE TI	CONSECUENCIA
Enlaces de Cableado	El daño o interrupción de la red de cableado estructurado provoca que los usuarios no puedan acceder a varios servicios como Internet, Intranet, información de unidades de red, así como también del servicio de impresión, copiado, escaneado y fax.
Equipos de Computación y Componentes	El daño o la falta de equipos de computación y dispositivos eléctricos y sus componentes provocan retraso en el trabajo de los miembros del Departamento de TI y de los usuarios de toda la compañía.
VNC	Impide tener acceso al control y asistencia remota a los equipos de informáticos la empresa.
Proyector	No permite proyectar imágenes o diapositivas que son regularmente usadas para conferencias.

Tabla 3.27: Consecuencias de la Interrupción de un Servicio de TI

3.3.2. FUNCIONES VITALES DEL NEGOCIO

De la Tabla 3.28 se puede indicar que las funciones vitales del negocio son las siguientes:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
Emisión	Recepción de Solicitudes de Póliza	3	0	3	2	8
	Emisión y envío de certificados de seguros	2	0	1	2	5
	Facturación a la compañía de seguros	2	3	1	1	7
	Pago de primas acreditado a la cuenta de la compañía de seguros	2	3	1	2	8
Renovación	Generación de la base de datos de clientes con pólizas a vencer	2	0	0	0	2
	Asignación de la base de clientes a cada ejecutivo	1	2	0	0	3
	Gestión para contactar al cliente	2	0	3	2	7
	Cotización de póliza de entre las distintas aseguradoras asociadas	2	3	2	2	9
	Emisión y envío de certificado de seguro en caso de haber acuerdo	3	0	1	1	5
	Ingreso de facturas de listado de pagos de producción mensual	2	3	0	0	5

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Pago de primas acreditado a la cuenta de la compañía de seguros	2	3	1	2	8
	Generación y envío de notificaciones finales a clientes con pólizas por vencer y que no han podido ser contactados o no desean el seguro	2	1	2	2	7
Cobranzas	Recepción de pólizas y valores correspondientes a los pagos de la póliza	3	3	2	0	8
	Generación de facturas	2	3	1	2	8
	Depósito de pagos de las pólizas	2	3	2	2	9
	Consolidación de cuentas	3	3	0	1	7
Siniestros	Notificación y registro de incidentes	1	1	3	2	7
	Asesoría y seguimiento de incidente	1	0	3	2	6
Dirección	Coordinar las tareas entre las áreas	0	0	0	0	0
	Evaluar el desempeño del personal	0	0	1	0	1

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Realizar el mejoramiento continuo de los procesos	0	0	0	2	2
	Atención de reclamos de clientes descontentos	2	0	3	1	6
	Control interno de los ingresos y egresos	3	3	0	0	6
	Planificación de recursos humanos	0	0	0	1	1
	Elaboración de rol de pagos	1	3	0	0	4
	Aprobación de adquisición de insumos	2	2	0	0	4
Gerencia	Negociaciones de los planes de seguros	2	0	0	3	5
	Presentación de informes de las actividades de la compañía a los socios	1	0	0	1	2
Asistencia Médica	Recepción y validación de solicitudes de seguros médicos.	3	0	2	1	6
	Registro del asegurado	1	0	1	0	2
	Emisión de certificado de seguros	2	0	1	1	4
	Emisión de facturas	2	3	1	2	8

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Gestión de reclamos de cobertura de medicinas, citas médicas, operaciones entre otros.	2	0	2	2	6
Recepción	Control del Libro Diario	3	0	0	1	4
	Control de Memorándumes emitidos	3	0	0	1	4
TI (Sistemas)	Creación de Usuarios	0	0	0	0	0
	Obtención de Backups	3	0	0	0	3
	Mantenimiento de Comunicaciones	3	0	3	3	9
	Mantenimiento de Hardware	2	0	0	0	2
	Mantenimiento de Software	1	0	0	0	1
	Adquisición de Equipos	1	0	0	0	1
	Adquisición de Software	1	0	0	0	1
	Soporte a Usuarios	1	0	2	0	3
	Capacitación a Usuarios	1	0	1	0	2
	Mantenimiento y soporte del sistema SIBROK	3	0	3	0	6
	Manejo de Cableado y equipos electrónicos	1	0	2	0	3
	Elaboración de reportes de producción	3	3	0	0	6

FUNCIÓN DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL			TOTAL
			FC	SC	PM	
	Ingreso de pólizas de seguro	3	3	1	0	7
	Renovación de seguros	3	3	1	2	9
	Depuración de la información	3	0	0	0	3

Tabla 3.28: Funciones Vitales del Negocio

La representación del significado de los colores presentados en la Tabla 3.28 se los indica en la Tabla 3.29.

COLOR	DESCRIPCIÓN
	En el Impacto Financiero se obtuvo un valor de 2 o 3.
	Si en el Impacto operacional existen al menos dos valores “Alto”.
	Si en el Impacto Operacional existen al menos un valor “Alto” y un valor “Medio”.
	(Procesos Críticos) Procesos que cumplen con las condiciones antes mencionadas.
	Funciones Vitales del Negocio

Tabla 3.29: Coloración de la Tabla de Funciones Vitales del Negocio

3.3.3. REQUISITOS DE DISPONIBILIDAD

A continuación se indican los Requisitos de Disponibilidad, los cuales son un extracto del Anexo 5: Requerimientos de Disponibilidad.

3.3.3.1. ALCANCE

En esta sección del documento se describe cada servicio de TI de la empresa RELIANCE, con la siguiente estructura:

- Descripción del servicio.
- Requerimientos del negocio: Describe las razones y necesidades del servicio de TI y en donde se alinea con las necesidades del negocio. Los requerimientos serán claros y estarán descritos en términos del negocio.
- Funciones vitales relacionadas con el servicio: las funciones vitales del negocio y los procesos con los que está relacionado el servicio.

3.3.3.2. RESUMEN DE DISPONIBILIDAD DE SERVICIO TI

En la Tabla 3.30 se representa un resumen de servicios TI de RELIANCE.

Servicio TI	Horas de Servicio	Tiempo de Recuperación	Capacidad para Adaptarse	Utilidad	Periodo de Mantenimiento
Microsoft Office	10/7	2 horas	Alta	Alta	Semestral
Outlook Express	10/7	3 horas	Alta	Alta	Semestral
Internet	24/7	1 hora	Baja	Alta	Semanal
Scanner	10/5	1 hora	Baja	Baja	Mensual
Impresora	10/5	1 hora	Baja	Baja	Mensual
Fotocopiadora	10/5	1 hora	Baja	Baja	Mensual
Fax	10/5	1 hora	Baja	Media Baja	Mensual
UPS (Alimentación Eléctrica Ininterrumpida)	24/7	4 horas	Baja	Alta	Semestral
SIBROK (Sistema Integrado de Brokers)	24/7	2 horas	Baja	Alta	Mensual

Servicio TI	Horas de Servicio	Tiempo de Recuperación	Capacidad para Adaptarse	Utilidad	Periodo de Mantenimiento
Intranet	24/7	1 hora	Medio	Alta	Mensual
Correo Electrónico	24/7	3 horas	Medio	Alta	Semanal
Servidor de Archivos	10/5	3 horas	Medio	Media Alta	Mensual
Antivirus	24/7	24 horas	Alta	Media Alta	Semanal
Adobe Reader	10/5	2 horas	Baja	Alta	Semestral
Enlaces de Cableado	24/7	2 horas	Baja	Alta	Semestral
Equipos de Computación y Componentes	24/7	2 horas	Medio	Alta	Semestral
Acceso y Control Remoto	24/7	24 horas	Alta	Media	Mensual
Proyector	10/5	24 horas	Baja	Baja	Semestral

Tabla 3.30: Resumen de Disponibilidad de Servicios TI de RELIANCE

3.3.3.3. REQUERIMIENTOS DE DISPONIBILIDAD

MICROSOFT OFFICE

Descripción del Servicio:

Suite de oficina con aplicaciones de procesamiento de textos, plantilla de cálculo y programa para presentaciones.

Requerimientos del Negocio:

- Procesador de texto, que permita llenar los formularios necesarios enviados por las aseguradoras, manejar el historial del cliente, redacción de cartas, oficios, notificaciones, informes.
- Debe permitir insertar imágenes de diversos formatos en cualquier parte del documento. Para poder retener información del cliente como la cedula

de identidad / pasaporte, el estado de los bienes asegurados, tener fotografías en el caso de siniestros.

- Hoja de cálculo que interactué en línea con el sistema SIBROK para la generación de reportes de producción, listado de clientes con pólizas a vencer por servicio/producto.

Fallos:

- No se puede abrir documentos por diferencias entre versiones.
- Si documentos que son sólo de lectura puede ser modificados por otros sin permiso.
- Pérdida de las modificaciones realizadas frente a una caída de la aplicación.
- Cambios en el formato del documento

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

OUTLOOK EXPRESS

Descripción del Servicio:

Aplicación de cliente de correo electrónico usado para la recepción y envío de correo electrónico tanto a nivel interno de la empresa como externo a la misma.

Requerimientos del Negocio:

- Cada asesor debe manejar su correo en su equipo asignado, se debe notificar de forma inmediata de correo entrante mediante la sincronización y descargar el correo electrónico.

- Enviar mensajes de texto y archivos adjuntos fácilmente de forma instantánea.
- Identificar la información visualmente.
- Que permita tener una estructura de carpetas para una mejor organización de la información.
- Realice búsquedas instantáneas en toda su información.
- Evite el correo no deseado y reduzca la exposición a sitios maliciosos.
- Ayude a garantizar la legitimidad del correo electrónico

Fallos:

- No se puede descargar los correos de bandeja de entrada.
- Los correos no pueden ser enviados.
- Llegan incompletos
- Retraso en el envío/recepción de mails
- Exceso de spam
- Bloqueo de contactos / mails

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

SCANNER

Descripción del Servicio:

Captura y digitalización de imágenes, documentos de texto y transferencia de los mismos a un ordenador.

Requerimientos del Negocio:

- Obtener capturas de imágenes y documentos con una buena calidad, que sean legibles.
- Permita escanear varios documentos colocándolos en una bandeja, es decir sin tener la necesidad de colocar hoja por hoja.
- Que permita guardar los documentos digitalizados como imagen, documento de Word, pdf.
- Que permita la selección de una sección del documento.
- Las capturas no lleven más de 1 minuto.
- Debe pasar encendida todo el tiempo durante la jornada de trabajo, por lo el consumo de energía debe ser bajo.

Fallos:

- Las imágenes no pueden ser guardadas en el ordenador.
- Sólo acepta un tipo de formato para guardar
- La captura es muy lenta, lleva más de 1 minuto.
- Hay problemas con el software empleado.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

IMPRESORA

Descripción del Servicio:

Presentación de información impresa en papel, tanto texto como gráficos.

Requerimientos del Negocio:

- Permitir escoger si la impresión es a blanco y negro o a color.
- Permita controlar el nivel de tinta utilizado.
- Permita la selección del tipo de papel (hojas membretadas, bond / recicladas) y esté disponible en las diferentes bandejas.
- Se puedan enviar varios documentos a la vez y se impriman todos sin problema.
- Que se puedan mandar a ejecutar varias acciones al mismo tiempo sin que cause conflicto.
- Permita tener un control del uso de los insumos.
- Debe pasar encendida todo el tiempo durante la jornada de trabajo, por lo el consumo de energía debe ser bajo.

Fallos:

- Se pierden documentos enviados de forma simultánea.
- Imprime a pesar de no tener papel
- Hay problemas con los cartuchos.
- Hay problemas con el software empleado.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

FOTOCOPIADORA

Descripción del Servicio:

Copiado en papel de un documento impreso.

Requerimientos del Negocio:

- Obtener capturas de imágenes y documentos con una buena calidad, que sean legibles.
- Permita escanear varios documentos colocándolos en una bandeja, es decir sin tener la necesidad de colocar hoja por hoja.
- Las capturas no lleven más de 1 minuto.
- Se pueda realizar impresiones a blanco y negro o color.
- Permita controlar el nivel de tinta utilizado.
- Debe pasar encendida todo el tiempo durante la jornada de trabajo, por lo el consumo de energía debe ser bajo.

Fallos:

- La captura es muy lenta.
- Imprime a pesar de no tener papel.
- Se atasca el papel.
- Hay problemas con los cartuchos.
- Hay problemas con el software empleado.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

FAX

Descripción del Servicio:

Copiado en papel de un documento impreso.

Requerimientos del Negocio:

- Manejo de fax entrante y saliente
- Reducido tiempo de procesamiento de fax
- Impresiones claras

Fallos:

- Pérdida de Fax en el envío y/o recepción
- Atascamiento de papel
- Las impresiones no son lo sufrientemente claras o imprime en blanco
- Desperdicio de papel

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

INTRANET

Descripción del Servicio:

Servicio de red interno que tiene como función principal compartir recursos informáticos aplicada a las necesidades del negocio para aplicaciones de captura, informes y consultas con el fin de facilitar la producción a nivel de grupo de trabajo

Requerimientos del Negocio:

- Cada equipo debe tener una IP fija, que facilite el acceso a la información y los servicios que requiere cada usuario.
- Los equipos deben estar conectados entre sí por una red de cableado.

- Restringir el acceso mediante usuarios y permisos a los servicios e información.
- Un sistema de gestión de red, el cual permita el control de prestaciones, problemas, seguridad, configuración debe permitir trabajar fuera del horario laboral de la organización, debe estar disponible 24/7.
- Compartir el uso de documentos en tiempo real rapidez en la toma de decisiones.
- Garantizar que los datos no sean comunicados incorrectamente es confiable.

Fallos:

- No se puede acceder remotamente a otro equipo.
- Hay servicios a los cuales no se puede acceder.

Funciones Vitales Relacionadas con este Servicio

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

INTERNET

Descripción del Servicio:

Red pública que permite la conexión con otras redes y usada la comunicación, búsqueda y transferencia de información. Esta red es provista por la empresa INTERACTIVE.

Requerimientos del Negocio:

- Redundancia y los balanceos de carga, balanceando las peticiones WEB, FTP, SMTP y POP.

- Baja latencia, al retardo (delay) que se dan en los paquetes debe ser bajo.

Fallos:

- El modem del proveedor no está funcionando, hay luces de tonalidad.
- No hay salida a internet desde los ordenadores.
- Las búsquedas, descargas se ejecutan muy lento.

Funciones Vitales Relacionadas con este Servicio:

- Sistemas

SIBROK (Sistema Integrado De Brokers)

Descripción del Servicio:

Sistema integrado que permite gestionar y administrar toda la información de las pólizas de seguros

Requerimientos del Negocio:

- Se tenga acceso a la base unificada de contactos, base única de nombres y direcciones (prospectos, clientes, aseguradoras, productores y grupos de empresas, entre otros).
- Posibilidad de acceder a la información de manera ágil e intuitiva, mediante la interface
- Permita segmentar la cartera de clientes y operaciones con fines estadísticos y de gestión.
- Emisión de Certificados de Cobertura y Orden de Emisión de Póliza, tanto para seguros nuevos como para endosos.
- Permita realizar la renovación de pólizas.
- Facturación o Contabilización de la póliza o endoso, con un plan de pagos configurable según cada necesidad.
- Permita una gestión Integral de Siniestros, para llevar un historial del cliente.

- Cuente con un módulo de consultas totalmente visual e intuitivo que ayude a los asesores en su labor diaria.
- Se puede acceder a estadísticas de producción.
- La información debe ser administrada por el responsable de la generación de la misma.

Fallos:

- No hay conexión con la base de datos.
- No se puede actualizar la información.
- Las consultas no están completas o no hay los suficientes criterios para generarlas.
- La aplicación no se ejecuta.
- No puede ingresar a la aplicación con su usuario.
- No se tiene los suficientes permisos.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

UPS (Alimentación Eléctrica Ininterrumpida)

Descripción del Servicio:

Sistema de alimentación de energía ininterrumpida, que permite proporcionar energía a un dispositivo en el caso de interrupción eléctrica.

Requerimientos del Negocio:

- Respaldar el trabajo que se está realizando al momento que ocurre el apagón, es decir dar un tiempo prudente para guardar el trabajo.

- Proveer la energía necesaria para seguir trabajando durante el restante de tiempo de la jornada de trabajo sin ningún problema.
- Los equipos indispensables para la ejecución de las tareas deben estar activos, por lo que permite conectar varios equipos indispensables.
- Las sobrecargas de energía a los equipos deben estar controladas, es decir se incluyen un regulador de voltaje.
- Protección de la línea telefónica ó el módem.

Fallos:

- La fuente de poder de los equipos ocasionalmente / frecuentemente se ven dañadas.
- Cuando se dan variaciones de voltaje suele apagarse los equipos.
- Frente a un apagón los equipos no permanecen el tiempo suficiente encendidos para guardar el trabajo.
- La energía proporcionada no abastece a los principales equipos para ejecutar las labores.
- La energía alterna se agota y no es suficiente para concluir la jornada laboral.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

CORREO ELECTRÓNICO

Descripción del Servicio:

Servicio de red que permite a los usuarios enviar y recibir mensajes electrónicos, así como también enviar y recibir archivos.

Requerimientos del Negocio:

- Tamaño buzón 80 Mb, en el caso de superar este límite, los nuevos mensajes no se podrán almacenar y serán devueltos.
- Tamaño máximo de un mensaje 10 Mb.
- Número máximo de destinatarios por mensaje 100.
- Servidores de correo que permitan autenticación TLS y conexiones seguras SSL
- Uso del buzón de correo, desde ordenadores internos y externos.
- Uso de clientes de correo con soporte POP3 y POP3 seguro conectándose al servidor y de clientes web.
- Medidas contra el correo basura
- Verificación de correo libre de virus.
- Chequeo de correo entrante para poder identificar mails que son spam.
- Configuración de las medidas a tomar con el spam, pueden ser eliminado automáticamente o marcado como spam para examinarlos posteriormente.
- Admitir la redirección de correo entrante a una cuenta que el usuario configure.
- Admitir auto-responder, con un mensaje pre configurado para un buzón determinado el cual es automáticamente enviado a la persona que te ha enviado un mail
- Gestión de Lista de Correo.
- Soporte para la sincronización de dispositivos móviles tipo Pocket PC y Smartphone vía ActiveSync.
- Soporte para la firma y encriptación de mensajes.
- Plataforma redundante que permite reducir el tiempo de indisponibilidad del servicio debido a labores de mantenimiento.
- Punto de acceso común para todas las configuraciones y todos los usuarios.

Fallos:

- Existe correos que no llegan a su destinatario.
- No se puede acceder con el cliente de correo y/o cliente web.

- Los correos son rebotados.
- No se da una correcta sincronización con dispositivos móviles.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

SERVIDOR DE ARCHIVOS

Descripción del Servicio:

Servidor que permite el acceso remoto a archivos almacenados en el mismo o directamente accesibles por éste.

Requerimientos del Negocio:

- La información más sensible debe estar centralizada.
- Actualización constante de la información en tiempo real.
- Respaldo periódico de la información (la más sensible semanalmente lo demás de forma mensual)
- Almacenamiento seguro y tolerante a fallos, mediante el uso de un RAID.
- Proporcione trabajar a usuario sobre el archivo como si estuviese en su escritorio esto debe ser transparente para el usuario.
- Organización de los archivos en una estructura de directorio jerárquica.
- Uso de criterios para definir el nombre de los documentos.

Fallos:

- La información no está actualizada.
- Existen duplicaciones de la información.
- No se puede localizar con facilidad los documentos.

- No se sigue las reglas para establecer el nombre de los documentos

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

ANTIVIRUS

Descripción del Servicio:

Aplicación informática que permite prevenir, detectar y eliminar virus informáticos.

Requerimientos del Negocio:

- Capacidad de detección y de reacción ante un nuevo virus, evitando la propagación y contagio.
- Actualización sistemática.
- Detección mínima de falsos positivos o falsos virus.
- No interferir con el rendimiento o desempeño normal de los equipos.
- Alertas disponibles en caso de detección, es decir una posible infección por las distintas vías de entrada (Internet, correo electrónico, red o discos).
- Capacidad de desinfección automática, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

Fallos:

- El equipo tiene un desempeño muy bajo, las aplicaciones no trabajan con rapidez.
- Se presenta constantemente un mensaje de problemas en el equipo.
- Solicita actualizaciones continuamente.
- No permite realizar un análisis de unidades externas.

- Se demora al realizar u análisis
- Los equipos están infectados.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

ADOBE READER

Descripción del Servicio:

Aplicación que permite abrir, guardar, imprimir y compartir documentos electrónicos.

Requerimientos del Negocio:

- Visualización e impresión de Formato de Documento Portátil
- Edición de documentos con formato pdf.
- Proporcionar seguridad a los documentos con formato pdf.
- Bajo consumo de recursos en el ordenador.

Fallos:

- No se puede visualizar documentos con formato pdf.
- No existe criterios de seguridad de los documentos.
- No puede generarse nuevos documentos pdf.
- Hay problemas para imprimir.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión

- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

ENLACES DE CABLEADO

Descripción del Servicio:

Red con cableado estructurado

Requerimientos del Negocio:

- Acceso a puntos de red de datos independientes para cada ordenador y servidor
- Admisión de una estructura escalable.
- Elaboración de un apropiado esquema de la estructura de acuerdo diseño de las instalaciones de la compañía.

Fallos:

- La conexión es intermitente.
- Hay periodos extensos en los que no hay red interna.
- No hay los suficientes puertos para conector los equipos.
- El cableado es constantemente dañado.

Funciones Vitales Relacionadas con este Servicio

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

EQUIPOS DE COMPUTACIÓN Y COMPONENTES

Descripción del Servicio:

Dispositivos eléctricos, electrónicos que permiten automatizar las tareas dentro de la organización, esto incluye a los dispositivos de almacenamiento extraíbles.

Requerimientos del Negocio:

- La capacidad de memoria RAM, disco duro, procesador de los equipos deben ser las mínimas necesarias para tener un alto desempeño.
- Los equipos deben estar dotados de los dispositivos necesarios que requiere la estructura de los servicios de TI.

Fallos:

- Los equipos son muy lentos.
- No soportan la resolución adecuado para las aplicaciones.
- Hay dispositivos que funciones de una manera extraña o simplemente no funcionan.

Funciones Vitales Relacionadas con este Servicio:

- Cobranzas
- Emisión
- Renovación
- Siniestros
- Asistencia Médica
- Sistemas

ACCESO Y CONTROL REMOTO

Descripción del Servicio:

- Aplicación de control y asistencia remota a los usuarios de la empresa.
- Requerimientos del negocio
- Provea un control total al ordenador.

- Brinde un acceso al ordenador sin interrumpir el trabajo de los asesores
- Ejecución de actualizaciones y mantenimiento del software del ordenador.
- Acceso remoto a los ordenadores dentro y fuera de la red interna.
- Proporcionar soporte a usuarios de forma remota.

Fallos:

- La comunicación es muy lenta.
- El acceso remoto es visible para los usuarios puesto que no les permite usar sus equipos.
- No se puede acceder.

Funciones Vitales Relacionadas con este Servicio:

- Sistemas

3.4. DISEÑO DE LA DISPONIBILIDAD

3.4.1. DISEÑO DE LA INFRAESTRUCTURA TI

3.4.1.1. ELEMENTOS DE LA RED

Los componentes que ayudan a la integración de esta infraestructura TI son los siguientes:

- Interfaces de red: Todas aquellas que han sido descritas en la Tabla 3.8.
- Servidor: PC que permite la administración de las cuentas de los usuarios registrados en la red de la organización. Para este caso se utiliza al PC “SERVIDOR”, descrito en la Tabla 3.3.
- Clientes: Todos los PC’s que son utilizados por los usuarios de la red, los cuales utilizan los recursos de red. Los PC’s y los cuales han sido descritos en la Tabla 3.3
- Switch: Componente descrito en la Tabla 3.6.
- Impresoras: Todos los componentes descritos en la Tabla 3.4 y Tabla 3.5.

- Sistemas Operativos: En el estado actual de la empresa el servidor cuenta ya con Windows Server 2003 R2, y para los clientes con Windows XP Professional.
- Cableado estructurado.

Se recomienda el uso de un router que asegura el enrutamiento de paquetes en la red, o bien determinar la ruta exacta que debería tomar el paquete de datos que se intercambia.

3.4.1.2. ADMINISTRACIÓN DE TI

Al momento la organización no cuenta con herramientas de software eficaces para la administración de TI, por lo que a continuación se recomienda los siguientes componentes que ayudarían al departamento de ti.

- Herramienta que permita controlar el inventario del equipo
    - OCS INVENTORY
- Herramientas para monitoreo de red
    - NAGIOS
    - MRTG (*Multi Router Traffic Grapher*)

3.4.1.3. ALMACENAMIENTO

Los componentes que ayudan al almacenamiento de la información son los siguientes:

- Distribución de datos en varios discos, se recomienda usar un RAID 1 en el servidor de aplicaciones.
- Herramienta de respaldo y recuperación, AcronisBackup Server, descrito en la Tabla 3.11.
- Unidades de almacenamiento en los PC de los usuarios, descrito en la Tabla 3.9.

3.4.1.4. IMPRESIÓN Y DIGITALIZACIÓN

Los componentes que ayudan en la impresión y digitalización son los siguientes:

- Impresoras, descritos anteriormente en la Tabla 3.4.
- Impresoras multifunción, descrita en la Tabla 3.5.

3.4.1.5. CONSIDERACIONES PARA EL HARDWARE Y SOFTWARE

3.4.1.5.1. CONSIDERACIONES DE HARDWARE

- Las características mínimas necesarias para los equipos clientes para satisfacer las necesidades del negocio son las siguientes:
    - requerimientos mínimos para clientes
    - Procesador: 2.0 GHz o más
    - Memoria (RAM): 1 GB
    - Espacio en Disco: 150 Gb o más
    - Pantalla (monitor):resolución de 1024x768
- Los requerimientos mínimos de hardware para el servidor de aplicaciones son los siguientes:
    - Procesador: 2.0 GHzo más
    - Memoria (RAM): 2 GB o más
    - Espacio en Disco: Dos discos de 500 Gb
    - Pantalla (monitor):resolución de 1024x768

- Los requerimientos mínimos de hardware para el servidor de administración de TI son los siguientes:
    - Procesador: 2.5 GHzo más
    - Memoria (RAM): 4 GB o más
    - Espacio en Disco: 500 Gb
    - Pantalla (monitor):resolución de 1024x768

3.4.1.5.2. CONSIDERACIONES DE SOFTWARE

Mantener las aplicaciones con las actualizaciones más importantes que brinde el proveedor.

Los beneficios que se obtiene son; acceder a las nuevas funciones, optimización de rendimiento de la aplicación, cerrar puertas traseras que permitan el ingreso de código malicioso.

Sistema Operativo:

- Clientes: Windows XP SP3. Se debe tratar de migrar a Windows 7 ya que Microsoft dará soporte hasta el 2014.
- Servidor: Windows Server 2003 R2 e instalados los últimos parches para mejorar la seguridad del servidor.

Herramientas ofimáticas:

- Microsoft Office: migrar debido a soporte

3.4.1.6. CONSIDERACIONES PARA EL ENTORNO DE LA INFRAESTRUCTURA DE TI

En la Tabla 3.31, se representan las consideraciones necesarias para la Sala Principal de Equipos Informáticos.

SALA PRINCIPAL DE EQUIPOS (Master Room)	
Acceso	Entrada controlada, uso de combinación/clave, tarjeta magnética, cámara de video.
Ubicación	Primera planta siempre que sea posible, sin agua, gas, químicos o riesgos de incendio en las cercanías es decir por encima, debajo o al lado del cuarto.
Visibilidad	No señalización, no ventanas exteriores.
Revestimiento	Revestimiento externo: impermeable, hermético, aislamiento

	acústico, resistente al fuego (0,5 horas a 4 horas dependiendo de la criticidad)
Equipo de Entrega	Deberían tomarse medidas adecuadas para la entrega y colocación de equipos grandes sensibles.
Piso Interno	Sellado
Planta Eléctrica	Fuente de alimentación ininterrumpible (UPS). El suministro eléctrico y la distribución, la manipulación de unidades de aire.

Tabla 3.31: Sala Principal de Equipos Informáticos[30]

En la Tabla 3.32, se representan las consideraciones necesarias para la Sala Equipos de Redes y Servidores.

SALA DE EQUIPOS DE REDES Y SERVIDORES	
Acceso	Entrada controlada, uso de combinación/clave, tarjeta magnética. En algunos casos los equipos se encuentren en las oficinas abiertas en bastidores con llave o gabinetes.
Temperatura	Entorno de oficina normal, pero si las habitaciones son cerradas o bloqueadas debe proporcionarse una ventilación adecuada.
Humedad	Entorno normal de oficina, controlado.
Calidad del aire	Entorno normal de oficina.
Power	Energía continua suministrada con una fuente de poder sustituta – UPS a la granja de servidores completa.
Piso Falso	Recomendada de 3 m mínima entre el suelo y el techo, con todos los cables asegurados en varios compartimentos.
Paredes interiores	Siempre que sea posible las paredes deben ser resistentes al fuego.
Detección /	Sistema de detección de incendios/humo normal de oficina.

[30] Office of Government Commerce (OGC); ITIL la Llave para la Gestión de los Servicios TI; Mejores Prácticas para la Provisión del Servicio; versión 3;2007; Appendix E: Environmental architectures and standards; 245

SALA DE EQUIPOS DE REDES Y SERVIDORES	
Prevención de incendio	
Detectores en el Entorno	Para el humo, energía, con capacidad de alarma sonora
Iluminación	Los niveles normales de iluminación de techo con luces de emergencia en caso de corte de energía.
Conexión a Tierra	Se debe proveer de conexión a tierra a los equipos. Y los botones de apagado claramente identificados.
Extinguidores de Fuego	Suficientes extintores de incendio eléctrico con señalización adecuada y procedimiento.
Vibración	Las vibraciones deben ser mínimas dentro de la zona
Interferencia Electromagnética	Interferencia mínima (1.5V/m campo de fuerza ambiente)
Instalaciones	Todos los equipos e instalaciones eléctricas deben ser suministrados e instalados por proveedores cualificados y normas adecuadas de salud y seguridad
Conexiones de Red	El equipo de campo debe ser de cable aislado con una capacidad adecuada para un crecimiento razonable. Todos los cables deben ser colocados y sujetos a las bandejas de cable adecuado.
Recuperación de Desastres	Completamente probado y los planes de recuperación deben desarrollarse de acuerdo al caso.

Tabla 3.32: Sala de Equipos de Redes y Servidores[31]

En la Tabla 3.32, se representan las consideraciones necesarias para el Entorno de Oficina.

[31]Office of Government Commerce (OGC); ITIL la Llave para la Gestión de los Servicios TI; Mejores Prácticas para la Provisión del Servicio; versión 3;2007; Appendix E: Environmental architectures and standards; 248

ENTORNO DE OFICINA	
Acceso	Todas las oficinas deben tener la seguridad de acceso adecuado según la empresa, la información y el equipo que está contenido dentro de ellas.
Iluminación, temperatura, humedad y calidad de aire.	Entorno normal, ambiente de la oficina cómoda y ordenada, conforme a la salud de la organización, seguridad y medio ambiente
Alimentación de Energía	Energía continua suministrada con una fuente de poder sustituta – UPS a la granja de servidores completa.
Piso Falso	Recomendada de 3 m mínima entre el suelo y el techo, con todos los cables asegurados en varios compartimentos.
Detección de incendios, prevención y extintores	Detección de incendios, prevención de humo, sistemas de detección de incendios, sistemas de alerta de intrusión si aquí están las principales concentraciones de los equipos. Suficientes extintores del tipo adecuado, con señalización adecuada y los procedimientos
Conexiones de Red	El espacio de oficinas preferentemente debe tener ser por cable con la capacidad adecuada para un crecimiento razonable. Todos los cables deben ser colocados y sujetos a las bandejas de cable adecuado. Todos los equipos de red deben estar protegidos en armarios o gabinetes de seguridad.
Recuperación de Desastres	Completamente probado y los planes de recuperación deben desarrollarse de acuerdo al caso.

Tabla 3.33: Entorno de Oficina[32]

[32] Office of Government Commerce (OGC); ITIL la Llave para la Gestión de los Servicios TI; Mejores Prácticas para la Provisión del Servicio; versión 3; 2007; Appendix E: Environmental architectures and standards; 248

3.4.1.7. ANÁLISIS DE PUNTOS INDIVIDUALES DE FALLO DE COMPONENTES (SPOF)

3.4.1.7.1. ANÁLISIS DEL IMPACTO DEL FALLO DE UN COMPONENTE (CFIA)

En la Figura 3.2 se indica un diagrama con los Elementos de Configuración (CI), los cuales determinan los componentes a ser analizados dentro de la Infraestructura TI.

En la Tabla 3.34, se representa mediante una matriz el tipo fallo del CI, dentro de la Infraestructura TI propuesta anteriormente.

La Tabla 3.35 contiene una matriz que representa a los Elementos de Configuración, y el efecto que produce en las diferentes áreas del negocio, y el total de usuarios que son afectados por la pérdida de servicios de TI, que ofrecen estos Elementos de Configuración.

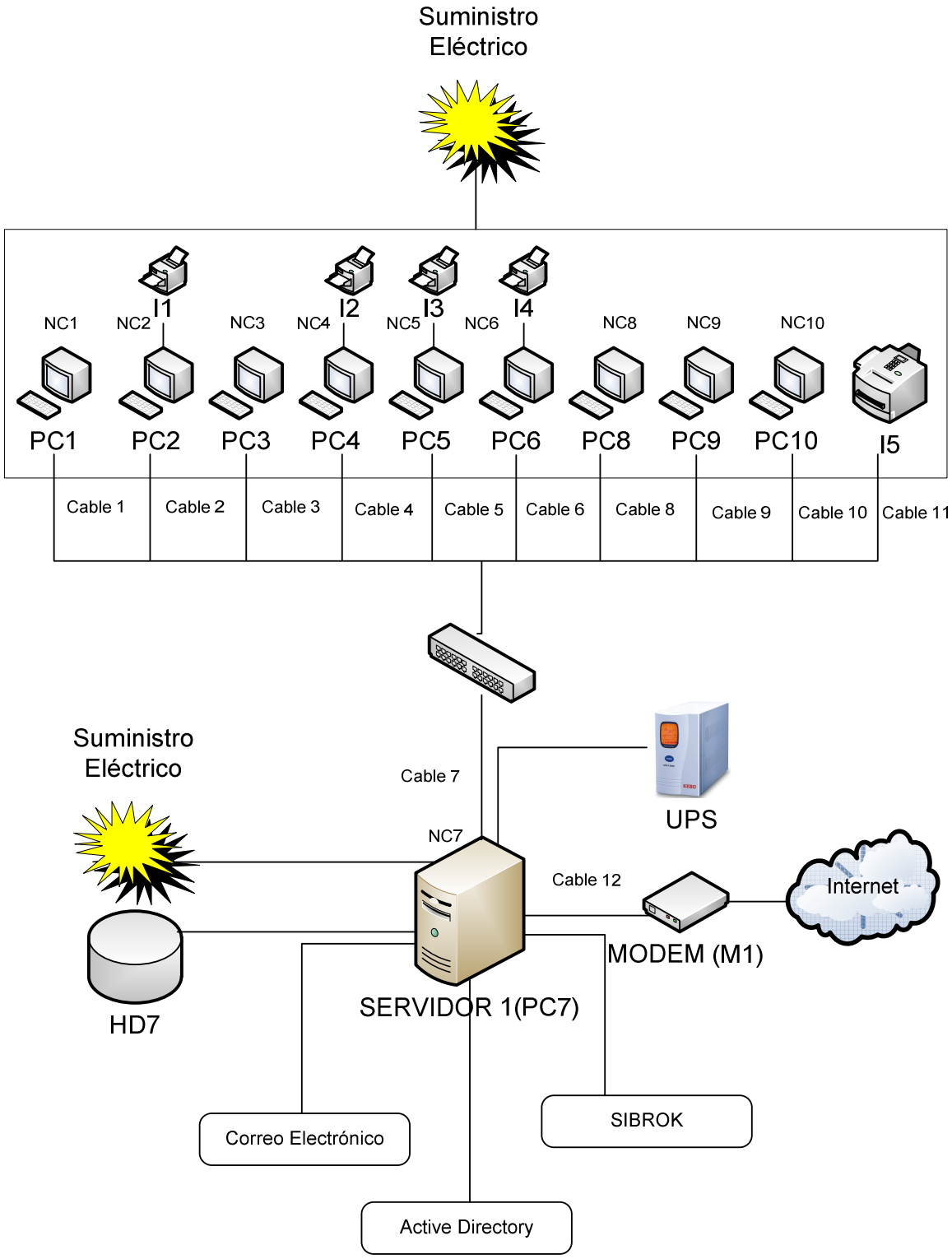

Figura 3.2: Configuración del Análisis del Impacto del Fallo de un Componente en RELIANCE[33]

[33] Estructura de la figura tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

CI	SERVICIOS																		
	Emisión de seguros	Envío de certificados de seguros	Pago de primas	Cotización de pólizas	Facturación	Notificaciones finales de Seguros	Pago de pólizas	Consolidación de cuentas	Registro de incidentes	Reclamos	Registro de ingresos y egresos	Rol de Pagos	Informes	Registro del asegurado	Administración de usuarios	Backups	Depuración de la información	Impresión-copiado-escáner	Internet
Suministro Eléctrico	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
UPS	X		X			X	X		X					X		X	X	A	X
PC1	X	X	X		A				A				A	A		X	A	A	
NC1	X	A	X		A				A				A	A		X	A	A	
CABLE 1	A	A	A		A				A				A	A		A	A	A	
PC2		X				A				A	A		A			X	A	A	
NC2		A				A				A	A		A			X	A	A	
CABLE 2		A				A				A	A		A			A	A	A	
PC3		X	X	X		X			X				A	A		X	X	A	
NC3		A	X	X		X			A				A	A		X	X	A	
CABLE 3		A	A	A		A			A				A	A		A	A	A	
PC4				X	X			X		A	X		A			X	X	A	
NC4				X	X			X		A	X		A			X	X	A	
CABLE 4				A	A			A		A	A		A			A	A	A	
PC5	X	A			X				X	X			A	X		X	X	A	
NC5	X	A			X				X	X			A	X		X	X	A	
CABLE 5	A	A			A				A	A			A	A		A	A	A	
PC6	X	X	X		A				A				A	A		X	A	A	
NC6	X	A	X		A				A				A	A		X	A	A	
CABLE 6	A	A	A		A				A				A	A		A	A	A	
PC7	X			X					X					X	X	X	X	A	X
NC7	X			X					X					X	X	X	X	A	X
CABLE 7	A			A					A					A	A	A	A	A	A
PC8	A	A				A			A				A	A	X	A	X	A	
NC8	A	A				A			A				A	A	X	A	X	A	
CABLE 8	A	A				A			A				A	A	A	A	A	A	
PC9				A		A				A	A	X	A			X	X	A	X
NC9				A		A				A	A	X	A			X	X	A	X
CABLE 9				A		A				A	A	A	A			A	A	A	A
PC10				A						A			A			X	X	A	X
NC10				A						A			A			X	X	A	X
CABLE 10				A						A			A			A	A	A	A
SWT1	X	X	X	X	X	X	X	X	X	A	X	X		X	X	X	X	X	X
M1																			X

CI	SERVICIOS																		
	Emisión de seguros	Envío de certificados de seguros	Pago de primas	Cotización de pólizas	Facturación	Notificaciones finales de Seguros	Pago de pólizas	Consolidación de cuentas	Registro de incidentes	Reclamos	Registro de ingresos y egresos	Rol de Pagos	Informes	Registro del asegurado	Administración de usuarios	Backups	Depuración de la información	Impresión-copiado-escáner	Internet
CABLE 12																			A
HD7	X			X					X					X	X	X	X	A	X
I1	A		A	A	A	A	A		A	A		A	A	A				A	
I2	A		A	A	A	A	A		A	A		A	A	A				A	
I3	A		A	A	A	A	A		A	A		A	A	A				A	
I4	A		A	A	A	A	A		A	A		A	A	A				A	
I5	A		A	A	A	A	A		A	A		A	A	A				A	
CABLE 11	A		A	A	A	A	A		A	A		A	A	A				A	
SW1	A	A				A			A	A			A						
SW2		X				X												A	
SW3																X	A		
SW4		A				A			A				A						
SW5	A	A				A			A	A			A						
SW6	A		A																
SW7															X	X			
SW8	X		X	X	X	X	X	X	X	X	X	X	X	X			X	X	
SW9		X				X												A	
SW10																			A
SW11																A			
SW12		X				X													
SW13	X		X	X	X	X	X	X	X	X	X	X	X	X			X	X	
SW14																A			
SW15	A	A				A			A				A						
SW16															X				
SW17	A	A				A			A	A			A						
S1	X		X	X		X	X		X					X		X	X		

Tabla 3.34: Matriz de Configuración del Análisis del Impacto del Fallo de un Componente de RELIANCE[34]

[34] Estructura de la tabla tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

CI	ÁREAS DEL NEGOCIO	USUARIOS FINALES AFECTADOS
Suministro Eléctrico	Todas	10
UPS	Todas	10
PC1	Renovación	1
NC1	Renovación	1
CABLE 1	Renovación	1
PC2	Recepción	1
NC2	Recepción	1
CABLE 2	Recepción	1
PC3	Emisión	1
NC3	Emisión	1
CABLE 3	Emisión	1
PC4	Cobranzas	1
NC4	Cobranzas	1
CABLE 4	Cobranzas	1
PC5	Asistencia Médica	1
NC5	Asistencia Médica	1
CABLE 5	Asistencia Médica	1
PC6	Renovación	1
NC6	Renovación	1
CABLE 6	Renovación	1
PC7	Todas	10
NC7	Todas	10
CABLE 7	Todas	10
PC8	TI Sistemas	1
NC8	TI Sistemas	1
CABLE 8	TI Sistemas	1
PC9	Dirección	1
NC9	Dirección	1
CABLE 9	Dirección	1
PC10	Gerencia	1
NC10	Gerencia	1
CABLE 10	Gerencia	1
SWT1	Todas	10
M1	Gerencia, Dirección	2
CABLE 12	Gerencia, Dirección	2
HD7	Todas	10
I1	Recepción	10
I2	Cobranzas	10
I3	Asistencia Médica	10
I4	Renovación	10

CI	ÁREAS DEL NEGOCIO	USUARIOS FINALES AFECTADOS
I5	Todas	10
CABLE 11	Todas	10
SW1	Todas	10
SW2	Todas	10
SW3	Todas	10
SW4	Todas	10
SW5	Todas	10
SW6	Gerencia, Dirección, Renovación, Emisión, TI Sistemas	9
SW7	Todas	10
SW8	Todas	10
SW9	Todas	10
SW10	Gerencia, Dirección	2
SW11	Todas	10
SW12	Todas	10
SW13	Todas	10
SW14	TI Sistemas	1
SW17	Todas	10
SW18	Todas	10
SW19	Todas	10
S1	Gerencia, Dirección, Renovación, Emisión, Cobranzas, TI Sistemas	9

Tabla 3.35: CFIA que Refleja las Relaciones entre Componentes, Áreas del Negocio y Usuarios Finales Afectados[35]

3.4.1.7.2. ANÁLISIS POR ÁRBOLES DE FALLOS (FTA)

Para el análisis por árboles de fallos se utilizan los siguientes operadores lógicos, como:

- AND ∩: El evento resultante sólo sucede cuando todos los sucesos entrantes ocurren simultáneamente.

[35] Estructura de la tabla tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

- OR : El evento resultante ocurre cuando suceden uno o más de los eventos entrantes.
- OR exclusivo : El evento resultante solamente ocurre cuando se satisface la condición de entrada.
- Inhibidor : El evento resultante solamente ocurre cuando no se satisface la condición de entrada. "[36]

A continuación en la Figura 3.3 y Figura 3.4 se representa el árbol de fallos con respecto a los servicios TI del Sistema SIBROK y Servidor de Correo Electrónico. Para el resto de servicios TI están representados en las figuras del Anexo 6: Análisis por Arboles de Fallo.

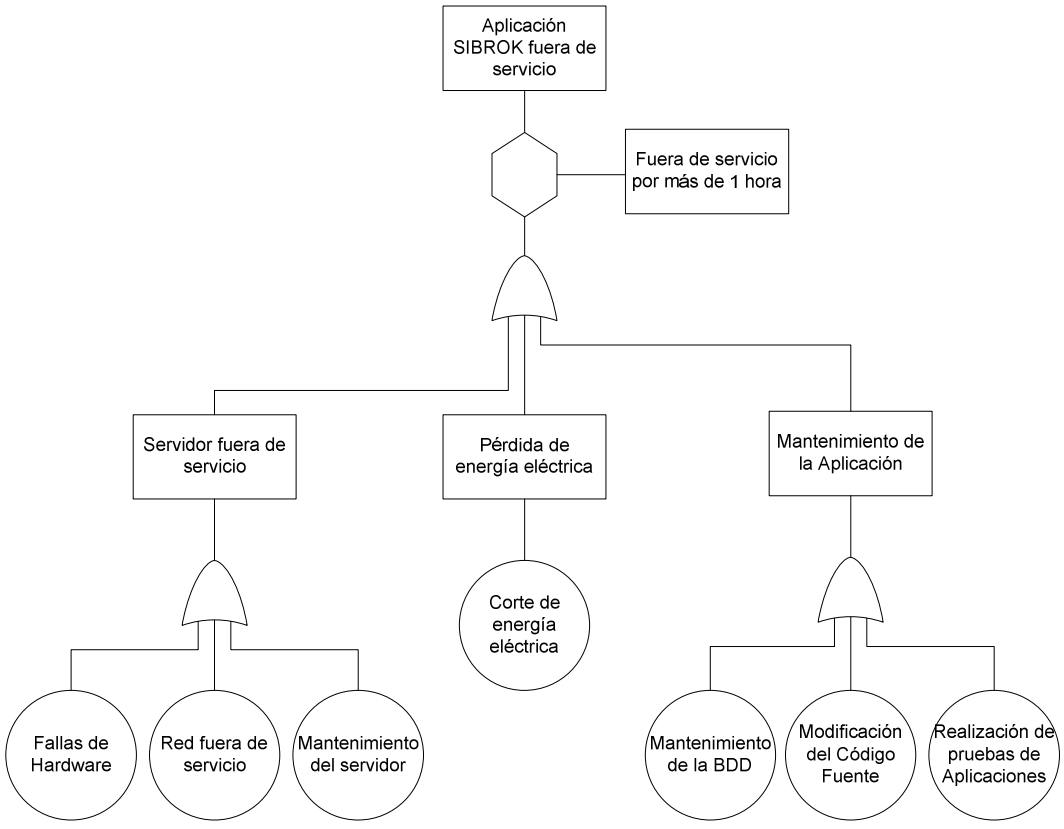

Figura 3.3: Análisis de Árbol de Fallos del Sistema SIBROK[37]

[36] Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

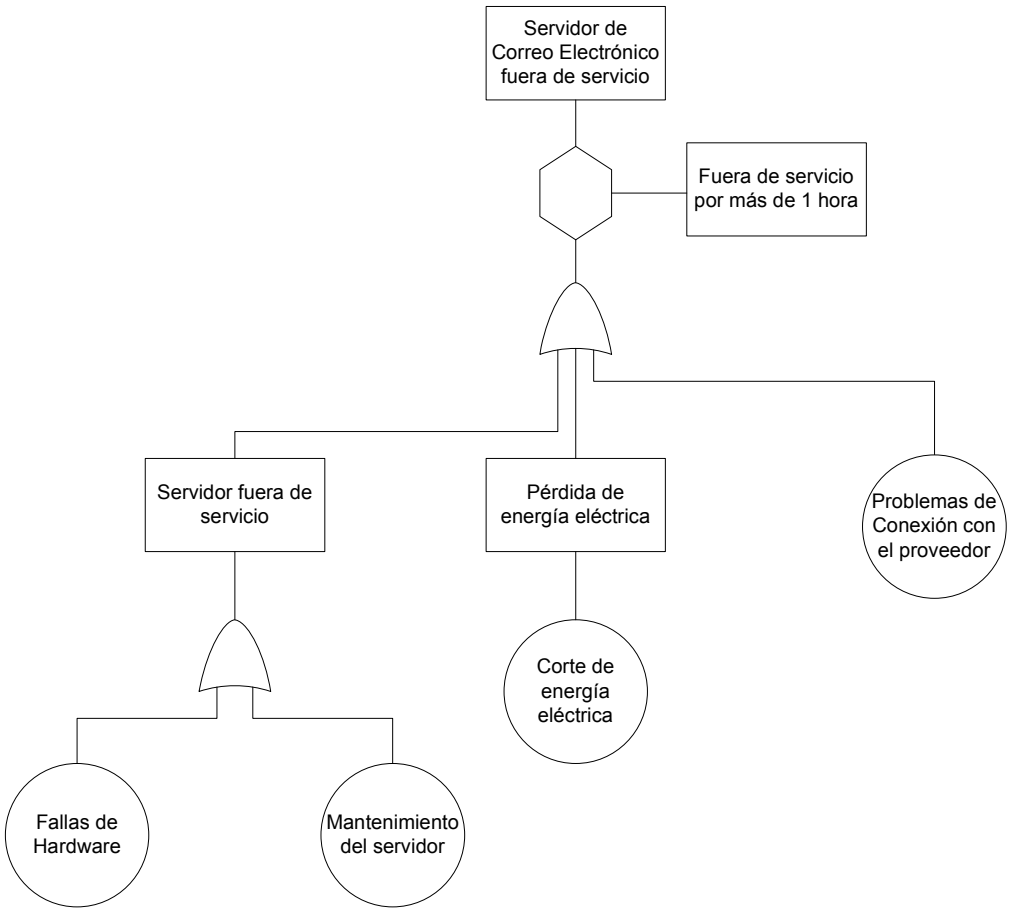

Figura 3.4: Análisis de Árbol de Fallos del Servidor de Correo Electrónico[38]

En las Figura 3.3 y Figura 3.4 se puede observar, que con la pérdida del suministro de la energía eléctrica, la mayoría de servicios TI pasan al estado de fuera de servicio, tal como se lo pudo demostrar en la sección anterior, en el Análisis de Impacto del Fallo de un Componente (CFIA).

También se puede observar que la pérdida del servicio de TI, en la mayoría de los casos se da debido a problemas de conexión en la red, fallas en el hardware y software, así como por tiempos de mantenimiento a los equipos y aplicaciones.

[37] Estructura de la Figura tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007
[38] Estructura de la Figura tomada de: Office of Government Commerce (OGC). ITIL la Llave para la Gestión de los Servicios TI. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007

3.4.1.8. GESTIÓN Y ANÁLISIS DE RIESGO

3.4.1.8.1. MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS (CRAMM)

3.4.1.8.1.1. VALORACIÓN DE ACTIVOS

Para la valoración de los activos se los da una puntuación de 1 a 10, donde 1 representa el menor valor que tendría un activo y 10 es el de mayor valoración como activo de la organización.

A continuación en la Tabla 3.36 se presenta una lista con todos los activos TI de la organización RELIANCE:

ACTIVO TI	VALORACIÓN
Microsoft Office	9
Outlook Express	9
Internet	2
Scanner	4
Impresora	10
Fotocopiadora	10
Fax	8
UPS	9
SIBROK (Sistema Integrado de Brokers)	10
Intranet	10
Correo Electrónico	9
Servidor	10
Antivirus	8
Adobe Reader	7
Enlaces de Cableado	10
Equipos de Computación y Componentes	8
Acceso y Control Remoto	6
Proyector	8
PC's clientes	9
Switch	9
Modem	8
Cableado estructurado	8
Interfaces de Red	8

ACTIVO TI	VALORACIÓN
Unidades de Almacenamiento	10

Tabla 3.36: Activos TI

3.4.1.8.1.2. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Para la identificación amenazas se las ha clasificado en amenazas de tipo Natural, Técnica y Humana. Para la valoración de las amenazas se les da una puntuación de 1 a 3, donde 1 representa la menor probabilidad de que ocurriese tal amenaza y 3 la mayor probabilidad de que ocurriese dicha amenaza.

A continuación en la Tabla 3.37 se presenta una lista con todas las amenazas que afectarían a los procesos de la organización.

TIPO DE AMENAZA	COD.	AMENAZA	VALOR
NATURAL	A1	Incendio	1
	A2	Terremoto/Temblor	1
	A3	Erupción Volcánica	1
TÉCNICA	A4	Interrupción de la energía eléctrica	2
	A5	Daño del Disco Duro del servidor o de los equipos clientes	3
	A6	Falla de los Servidores	3
	A7	Virus informático	3
	A8	Recalentamiento de los equipos	2
	A9	Problemas de Conexión	2
	A10	Fallas o daño en la red	3
	A11	Falta de espacio en almacenamiento de datos en los discos duros el servidor y los clientes	1
	A12	Falla o daño en el hardware de los equipos	3
	A13	Configuración incorrecta en las aplicaciones	2
	A14	Actualización incorrecta de las aplicaciones	1
	A15	Incorrecta validación de los datos en la base de datos del sistema SIBROK	3
	A16	Sobredimensionamiento en el número de equipos que forman parte de la red	2

TIPO DE AMENAZA	COD.	AMENAZA	VALOR
	A17	Falta de medios físicos para el respaldo de los datos	2
	A18	Problemas de validación de la información recibida por parte del banco	2
	A19	Falta de material para el mantenimiento de los equipos	1
	A20	Caída del servidor de la aplicación SIBROK	3
	A21	Caída del servidor de correo electrónico	3
HUMANA	A22	Hackers	3
	A23	Virus de Computadoras	3
	A24	Robo	3
	A25	Vandalismo	2
	A26	Daño de equipos por accidentes en el trabajo	2
	A27	Falta de capacitación en TI	1

Tabla 3.37: Tipos de Amenazas

3.4.1.8.1.3. IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES

Para la valoración de las vulnerabilidades se les da una puntuación de 1 a 3, donde 1 representa el menor impacto que tendría una amenaza si esta ocurriese y 3 representa el mayor impacto que tendría una amenaza si ocurriese.

A continuación en la Tabla 3.38 se presenta una lista con todas las vulnerabilidades que afectarían a los procesos de la organización.

AMENAZA	VULNERABILIDAD		
	CÓD.	Descripción	Valor
Incendio	V1	Pérdida de equipos, información física y lógica, pérdida de las comunicaciones	3
Terremoto /Temblor	V2	Pérdida de equipos, información física y lógica, pérdida de las comunicaciones	2

AMENAZA	VULNERABILIDAD		
	CÓD.	Descripción	Valor
Erupción Volcánica	V3	Pérdida de equipos, información física y lógica, pérdida de las comunicaciones	3
Interrupción de la energía eléctrica	V4	Pérdida de información en las horas laborables	3
		Retraso en las actividades	
Daño del Disco Duro del servidor o de los equipos clientes	V5	Pérdida de toda la información, así como de sus respectivos respaldos	3
Falla de los Servidores	V6	Pérdida de acceso a la información	3
		Pérdida de toda la información, así como de sus respectivos respaldos	
Virus informático	V7	Pérdida de información y/o archivos	3
		Modificaciones de archivos	
Recalentamiento de los equipos	V8	Retraso en las actividades	1
Problemas de Conexión en la red	V9	Pérdida de acceso a la información en los servidores	2
		Problemas de comunicación entre las estaciones de trabajo	
Falta de espacio en almacenamiento de datos en los discos duros el servidor y los clientes	V10	Pérdida de la nueva información generada	3
Falla o daño en el hardware de los equipos	V11	Pérdida de información almacenada en el equipo	3
		Retraso en las actividades	
Configuración incorrecta en las aplicaciones	V12	Retraso en las actividades	1
Actualización incorrecta de las aplicaciones	V13	Retraso en las actividades	1
Incorrecta validación de los datos en la base de datos del sistema SIBROK	V14	Información no confiable del sistema SIBROK	3
Sobredimensionamiento en el número de equipos que forman parte de la red	V15	Pérdida de acceso a la información en los servidores	2
		Problemas de comunicación entre las estaciones de trabajo	

AMENAZA	VULNERABILIDAD		
	CÓD.	Descripción	Valor
Falta de medios físicos para el respaldo de los datos	V16	Pérdida de información almacenada en los equipos	2
Problemas de validación de la información recibida por parte del banco	V17	Información no confiable del sistema SIBROK	2
Falta de material para el mantenimiento de los equipos	V18	Elevado tiempo de recuperación de los equipos	1
Caída del servidor de la aplicación SIBROK	V19	Indisponibilidad de la información para las diferentes áreas de la organización	3
Caída del servidor de correo electrónico	V20	Indisponibilidad de la información	3
		Indisponibilidad en el envío y recepción de solicitudes y valoraciones de pólizas de seguros	
Hackers	V22	Robo de la información	3
Virus de Computadoras	V23	Pérdida de información y/o archivos	3
		Modificaciones de archivos	
Robo	V24	Pérdida de equipos, información física y lógica, pérdida de las comunicaciones	3
Vandalismo	V25	Pérdida de equipos	2
Daño de equipos por accidentes en el trabajo	V26	Pérdida de equipos	2
Falta de capacitación en TI	V27	Retraso en las actividades	1

Tabla 3.38: Vulnerabilidades

3.4.1.8.1.4. EVALUACIÓN DE NIVELES DE RIESGOS

A continuación en la Tabla 3.39 se representa la probabilidad de que un riesgo ocurra en la organización, con respecto al servicio TI del sistema SIBROK. La Tabla 3.39 es un extracto del Anexo 7: Evaluación de Niveles de Riesgo.

ACTIVO TI	VALOR	AMENAZA	VALOR	VULNERABILIDAD	VALOR	RIESGO
SIBROK (Sistema Integrado de Brokers)	10	A1	1	V1	3	30
		A2	1	V2	2	20
		A3	1	V3	3	30
		A4	2	V4	3	60
		A5	3	V5	3	90
		A6	3	V6	3	90
		A7	3	V7	3	90
		A8	2	V8	1	20
		A9	2	V9	2	40
		A10	1	V10	3	30
		A11	3	V11	3	90
		A12	2	V12	1	20
		A13	1	V13	1	10
		A14	3	V14	3	90
		A15	2	V15	2	40
		A16	2	V16	2	40
		A17	2	V17	2	40
		A18	1	V18	1	10
		A19	3	V19	3	90
		A20	3	V20	3	90
		A22	3	V22	3	90
		A23	3	V23	3	90
		A24	3	V24	3	90
		A25	2	V25	2	40
		A26	2	V26	2	40
		A27	1	V27	1	10

Tabla 3.39: Evaluación de Niveles de Riesgos

Como se puede observar en la Tabla 3.39, los valores de los niveles de riesgos para el activo del sistema SIBROK, son valores muy altos llegando a tener un nivel de riesgo de hasta 90 y un nivel de riesgo mínimo de 10. Para el caso del valor de riesgo igual a 90 se hace referencia a la probabilidad de que la organización tenga un mayor impacto en sus procesos si los servidores llegasen a

estar fuera de servicio, en si el servidor que almacena al sistema SIBROK, también se tendría un mayor problema si al servidor es propenso a ataques de virus informáticos. Para el caso del valor de nivel de riesgo de 10, sin motivo alguno de descartarle, este tendría un menor impacto en los procesos del negocio, debido a que la capacitación de los usuarios para el uso de este sistemas es realizado por el propio personal del departamento de TI de la organización.

3.4.1.8.1.5. OPCIONES DE CONTROL DE RIESGOS

En la Tabla 3.40, se representa los controles de riesgo que permitirían reducir el impacto que tendría este en la organización, si llegase a ocurrir.

AMENAZA	CONTROL DE RIESGO	OPCIONES DE CONTROL
Incendio	Alarma contra incendios y extintores	Reducción del riesgo
	Seguro contra incendio	Transferencia del riesgo
	Protección de cuartos fríos con material aislante	Anulación del riesgo
	Equipos informáticos de respaldo.	Reducción del riesgo
Terremoto / Temblor	Seguro contra terremotos	Transferencia del riesgo
	Equipos informáticos de respaldo.	Reducción del riesgo
Erupción Volcánica	Seguro contra eventos volcánicos	Transferencia del riesgo
	Equipos informáticos de respaldo.	Reducción del riesgo
Interrupción de la energía eléctrica	Equipos de suministro alterno de energía eléctrica	Reducción del riesgo
Daño del Disco Duro del servidor o de los equipos clientes	Respaldos de información en CD-RW, DVD-RW, HD HARD DISC extraíbles, flash memory	Reducción del riesgo

AMENAZA	CONTROL DE RIESGO	OPCIONES DE CONTROL
	Respaldo de Información en otros servidores en línea	Reducción del riesgo
	Discos RAID	Reducción del riesgo
Falla de los Servidores	Disposición de servidores secundarios	Reducción del riesgo
	Respaldos de información en CD-RW, DVD-RW, HD HARD DISC extraíbles, flash memory	Reducción del riesgo
	Discos RAID	Reducción del riesgo
Virus informático	Programas Antivirus	Reducción del riesgo
	Firewall	Reducción del riesgo
	Capacitación a usuarios	Reducción del riesgo
	Controles para el uso Correo Electrónico	Reducción del riesgo
	Respaldos de información en CD-RW, DVD-RW, HD HARD DISC extraíbles, flash memory	Reducción del riesgo
	Plan de seguridad de datos	Reducción del riesgo
Recalentamiento de los equipos	Sistema de aire acondicionado	Anulación del riesgo
	Seguro técnico de los equipos	Transferencia del riesgo
	Sistema de control de flujo de energía eléctrica	Reducción del riesgo
Problemas de Conexión	Mantenimiento de la estructura de la red	Reducción del riesgo
	Aplicaciones de administración de la red	Reducción del riesgo
Fallas o daño en la red	Mantenimiento de la estructura de la red	Reducción del riesgo
Falta de espacio en almacenamiento de	Disposición de servidores secundarios	Reducción del riesgo

AMENAZA	CONTROL DE RIESGO	OPCIONES DE CONTROL
datos en los discos duros el servidor y los clientes	CD-RW, DVD-RW, HD HARD DISC extraíbles, flash memory	Reducción del riesgo
	Discos RAID	Reducción del riesgo
Falla o daño en el hardware de los equipos	Mantenimiento de Hardware y Software	Reducción del riesgo
	Seguro y garantías de hardware	Transferencia del riesgo
Configuración incorrecta en las aplicaciones	Manual de aplicaciones	Anulación del riesgo
Actualización incorrecta de las aplicaciones	Manual de aplicaciones	Anulación del riesgo
Incorrecta validación de los datos en la base de datos del sistema SIBROK	Archivos con formato para los datos	Reducción del riesgo
	Scripts que permitan determinar errores en los datos proporcionados	Reducción del riesgo
Sobredimensionamiento en el número de equipos que forman parte de la red	Switch con mayor número de puertos	Anulación del riesgo
	Planes de continuidad para el funcionamiento de la red	Reducción del riesgo
Falta de medios físicos para el respaldo de los datos	CD-RW, DVD-RW, HD HARD DISC extraíbles, flash memory	Reducción del riesgo
	Discos RAID	Reducción del riesgo
Problemas de validación de la información recibida por parte del banco	Archivos con formato para los datos	Reducción del riesgo
	Scripts que permitan determinar errores en los datos proporcionados	Reducción del riesgo

AMENAZA	CONTROL DE RIESGO	OPCIONES DE CONTROL
Falta de material para el mantenimiento de los equipos	Inventario mensual del material TI disponible	Anulación del riesgo
Caída del servidor de la aplicación SIBROK	Servidor de respaldo	Reducción del riesgo
Caída del servidor de correo electrónico	Servidor de respaldo	Reducción del riesgo
Hackers	Firewall	Reducción del riesgo
	Aplicaciones de protección contra pishing	Reducción del riesgo
	Aplicaciones de monitoreo de la red: sniffer	Reducción del riesgo
	Correcta configuración del servicio de correo electrónico	Reducción del riesgo
	Plan de seguridad de datos	Reducción del riesgo
Robo	Seguro contra robos	Transferencia del riesgo
	Equipos informáticos de respaldo.	Reducción del riesgo
	Plan de seguridad de datos	Reducción del riesgo
Vandalismo	Seguro de los equipos	Transferencia del riesgo
Daño de equipos por accidentes en el trabajo	Sanciones por negligencia	Reducción del riesgo
Falta de capacitación en TI	Capacitación de los usuarios en los servicios TI	Reducción del riesgo

Tabla 3.40: Opciones de Control de Riesgos

3.5. DISEÑO DE LA RECUPERACIÓN

3.5.1. ELEMENTOS PRINCIPALES DEL DISEÑO DE LA RECUPERACIÓN

A continuación se detallan los elementos principales del Diseño de la Recuperación, de acuerdo a las fases por las que pasa un incidente.

- Comienzo del incidente.
- Detección del incidente.
- Diagnóstico del incidente.
- Reparación del componente.
- Recuperación del componente.
- Restauración (y comprobación) del servicio.

Cada fase tienen un tiempo de duración que influye en el tiempo total de inactividad experimentado por el usuario, usando estos tiempos se pude identificar en cual fase se está tomando más tiempo, posibles áreas de ineficiencia, unas herramienta y scripts de diagnóstico deficientes, unos procedimientos de escalado poco claros (que retrasan la reasignación de la tarea al grupo de soporte técnico o proveedor apropiado) o la falta de una documentación operacional completa.

3.5.2. GESTIÓN DE SISTEMAS

En la sección 3.2.1.2 del Capítulo 3 Administración de TI, se enuncian herramientas que dan apoyo a la Organización de TI, las mismas que pueden ser utilizadas en la Gestión de Sistemas.

3.5.3. CAPTURA DE DATOS PARA EL DIAGNÓSTICO

En la Tabla 3.41 se presenta una lista con las principales métricas a tomar de los componentes de TI.

OBJETO	CONTADORES	VALORES UMBRALES

		Servidor de Aplicaciones	Servidor de Aplicaciones	PC
Procesador	% Tiempo de procesador	85	85	70
	%Tiempo privilegiado	75	75	
	Interrupciones/seg	1500	<1500	
Disco Físico	%Tiempo de lectura de disco	25	75	25
	%Tiempo de escritura en disco			
	Media en segundos/transferencia	< = 0,3 seg.	< = 0,3 seg.	< = 0,3 seg.
	Longitud media de la cola de disco	< = 2	< = 2	< = 2
	Bytes leídos y escritos/seg.	50%	50%	50%
Disco Lógico	% Espacio libre.	25	75	75
Red	% de utilización de la red	30 – 40	30 – 40	20 – 30
Caché	% de aciertos en mapas de datos.	> = 90%	> = 90%	> = 90%
Memoria	Lecturas de páginas/segundo.	5 – 10	5 – 10	5 – 10
	Bytes disponibles.	Mínimo 4MB	Mínimo 4MB	
	Bytes Comprometidos	Menor a la RAM	Menor a la RAM	Menor a la RAM
	% de Uso de la RAM	80%	80%	80%
	Bytes de memoria no paginable.	< = 50 % RAM		
Archivo de paginación	% de uso		99%	

Tabla 3.41: Métricas de Componentes de TI

El tiempo de caída adicional necesario para capturar los datos debe incluirse en las métricas de tiempo de recuperación documentado para cada uno de los componentes TI, se encuentra en el Anexo 5: Requerimientos de Disponibilidad.

3.5.4. NECESIDADES DE RECUPERACIÓN Y “BACKUP”

En la Tabla 3.42 se listan las necesidades de recuperación y “backup” de los componentes en que se basan los servicios TI, estas necesidades contemplan el hardware, software y datos.

SERVICIO DE TI	CRITERIOS DE RECUPERACIÓN
Microsoft Office	• Tener un respaldo del instalador con la versión empleada. • Recuperar los últimos archivos recuperados por el sistema.
Outlook Express	• Recuperar la organización de correos en el cliente del usuario. • Los correos de los últimos seis meses dentro de la estructura. • Elaborar un respaldo semanal del cliente correo.
Internet	• Reemplazo del modem provisto por el proveedor de internet
Scanner	• Solicitar al proveedor un reemplazo con las mimas características o similares al dispositivo.
Impresora	
Fotocopiadora	
Fax	
UPS	
SIBROK (Sistema Integrado de Brokers)	• Tener un respaldo del instalador con la versión empleada para el servidor y clientes • Plan de configuración del servidor y clientes. • Restaurar la base datos con el respaldo más reciente de la semana. • Un servidor de reemplazo con las características del plan de configuración.
Intranet	• Esquema de la red. • Servidor de LADP de reemplazo con las características adecuadas. • Dispositivos de conexión

SERVICIO DE TI	CRITERIOS DE RECUPERACIÓN
Correo Electrónico	• Tener un respaldo del instalador con la versión empleada para la conversión de dominio. • Plan de configuración de Lansuite. • Respaldo de los correos enviados y recibidos de los últimos 6 meses.
Servidor de Archivos	• Tener un respaldo del instalador con la versión empleada. • Plan de configuración del servidor y clientes. • Restaurar la información de los últimos 5 años.
Antivirus	• Tener un respaldo del instalador con la versión empleada. • Plan de configuración para los distintos dispositivos.
Adobe Reader	• Tener un respaldo del instalador con la versión empleada.
Enlaces de Cableado	• Tener el diagrama de diseño de la instalación. • Suministros: Cable CAT 5,
Equipos de Computación y Componentes	• Disponer de componentes de reservas, partir del inventario realizado de cada mes.
Acceso y Control Remoto (VNC)	• Mantener las IP internas y externas de los distintos equipos y servidores.

Tabla 3.42: Necesidades de Recuperación y Backup

3.5.5. MÉTRICAS DE RECUPERACIÓN

3.5.6. MÉTRICAS DE TIEMPO

Los parámetros que se muestran a continuación se evaluarán en función del tiempo.

- Tiempo de obtención de un servidor con capacidades similares al afectado: tiempo que transcurre desde que se ha solicitado al proveedor un equipo o recurso hasta que es entregado.

- Tiempo de instalación y configuración de software base en servidores: Tiempo que transcurre desde que inicia hasta que finaliza la instalación del sistema operativo utilizado en RELIANCE para los servidores, la base de datos requerida para el funcionamiento de las aplicaciones.
- Tiempo de instalación y configuración de aplicaciones en las pc de los usuarios: Tiempo que transcurre desde que inicia hasta que finaliza la instalación del sistema operativo utilizado en RELIANCE para las pc y los servicios necesarios para cada área descritas en la Tabla 1.4.
- Tiempo de Instalación y configuración de Impresoras: Tiempo que toma instalar un aproximado de 2 impresoras.
- Tiempo de Instalación y configuración de SIBROK): Tiempo que transcurre desde que se instala y configura la aplicación en el servidor.
- Tiempo para cargar el backup: Tiempo que transcurre desde que inicia hasta que finaliza la obtención del backup.
- Tiempo para validar los permisos de usuario: Tiempo que toma revisar los permisos para validador acceso según el perfil.
- Tiempo para verificar el buen funcionamiento del servicio: verificar que los datos estén completos y que sean confiables para su utilización.
- Tiempo para levar la topología de red: es el tiempo necesario para tender el cableado estructurado en la Empresa.
- Tiempo para instalar y configurar el router/switch: Tiempo que transcurre desde que se instala y configura el router/switch.
- Total Tiempo de recuperación: Tiempo total que ha transcurrido desde el inicio hasta el final de la recuperación. Suma de los tiempos anteriores.

3.5.7. MÉTRICAS DE COSTOS

Los parámetros que se muestran a continuación se establecen en función de los costos.

- Costo de componentes de TI: costo en dólares del componente de TI cambiado.

- Costo de un servidor con capacidades similares al servidor afectado: Costo
- en dólares de un servidor de las mismas capacidades del servidor que ha sufrido el daño.
- Costo de consultoría de Proveedores en caso de haber utilizado este servicio: costo de la evaluación y asesoría que realizan los proveedores en caso de daños que TI no pueda resolver.
- Total Costo de recuperación: el total de costo de recuperación en dólares. Suma de los costos incurridos para la recuperación del servicio.

3.5.8. MÉTRICAS DE EFECTIVIDAD DEL PLAN DE RECUPERACIÓN

Los parámetros de efectividad se muestran a continuación:

- Tiempo de Paralización de Operaciones del Negocio: Tiempo que el incidente/desastre ha afectado al negocio manteniendo el o los servicios paralizados.
- Número de procesos críticos afectados por el desastre: Número de procesos críticos del negocio que se ven afectados por la paralización de servicios.
- Tiempo de retrasos de trabajo: Los retrasos de trabajo que han sufrido los usuarios a causa de la paralización de los servicios.
- Número de usuarios afectados por el desastre: Número de usuarios que se ven afectados por la paralización de servicios.
- Esfuerzo invertido para la recuperación: El esfuerzo medido en horas/hombre para la recuperación.
- Confiabilidad e Integridad de la información recuperada: medido en porcentaje.
- Número de recursos de personal empleados para la recuperación: número de personas que se necesitaron para la recuperación, tanto los que fueron considerados en el plan de recuperación como personal adicional.
- Maximum Tolerable Downtimes (MTD): El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.

- RTO (Recovery Time Objective): El tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la caída del servicio.
- WRT (Work Recovery Time): Indica el tiempo disponible para recuperar los datos perdidos, trabajo retrasado y datos capturados manualmente durante la caída.
- RPO (Recovery Point Objective): Es la magnitud de datos perdidos que un proceso del negocio puede tolerar.

3.5.9. RESTAURACIÓN Y COMPROBACIÓN DEL SERVICIO

Se considera que un incidente está cerrado cuando se haya restaurado el servicio y restablecido el funcionamiento normal del negocio. Una vez finalizada la restauración del servicio se debe comprobar que el servicio restaurado esté funcionando correctamente para que le personal técnico implicado en el incidente pueda corregir antes de retirarse.

3.6. CONSIDERACIONES DE SEGURIDAD

A continuación para las consideraciones de la seguridad en los siguientes puntos, se presenta un extracto de la información presente en el Anexo 8: Consideraciones de Seguridad - Estándar Internacional ISO/IEC 17799.

3.6.1. SEGURIDAD DE LA INFORMACIÓN

Para la seguridad de la información se debe:

a) Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información.
b) identificar cómo manejar las no-conformidades.
c) Aprobar las metodologías y procesos para la seguridad de la información.
d) Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas.

e) Evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información.
f) Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.
g) Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información.

3.6.2. SEGURIDAD FÍSICA Y AMBIENTAL

Para la seguridad física y ambiental se debe tener en cuenta que:

a) Los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser físicamente sólidos, es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado.
b) Cuando sea aplicable, se debieran elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental.
c) Se debiera registrar la fecha y la hora de entrada y salida de los visitantes.
d) El acceso a áreas donde se procesa o almacena información sensible se debiera controlar y restringir sólo a personas autorizadas; se debieran utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos.
e) Se debiera requerir que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible.
f) Al personal de servicio de apoyo de terceros se le debiera otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial.
g) Los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario.

3.6.3. SEGURIDAD DE LOS EQUIPOS

Para los equipos de seguridad se debe tener en cuenta que:

a) El equipo se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo.
b) Los medios de procesamiento de la información que manejan datos confidenciales debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso.
c) Se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
d) Se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información.
e) Se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.
f) Se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.
g) Se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial.

3.6.4. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

Para el procesamiento de las operaciones se debe tener en cuenta que:

a) Copia de seguridad o respaldo.
b) Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.

c) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
d) Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
e) Instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos.
f) Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.
g) Gestión de la información del rastro de auditoría y registro del sistema.

3.6.5. RESPALDO O BACK-UP

Para el respaldo de la información se debe tener en cuenta que:

a) Se debiera definir el nivel necesario de respaldo de la información.
b) Se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.
c) La extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización.
d) Las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
e) La información de respaldo se le debiera dar el nivel de protección física y ambiental adecuados.
f) Los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.
g) Los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser

completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

h) En situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

3.6.6. SEGURIDAD DE LA RED

Para la seguridad en la red se debe tener en cuenta que:

a) Cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo.
b) Se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario.
c) Se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasa a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados.
d) Se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.
e) Las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.
f) La tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red.
g) Parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red.

3.6.7. MONITOREO

Para las actividades de monitoreo se debe:

a) Utilizar IDs.
b) Fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida.

c) Identidad o ubicación de la identidad.
d) Registros de intentos de acceso fallidos y rechazados al sistema.
e) Registros de intentos de acceso fallidos y rechazados a la data y otros recursos.
f) Cambios en la configuración del sistema.
g) Uso de privilegios.
h) Uso de las utilidades y aplicaciones del sistema.
i) Archivos a los cuales se tuvo acceso y los tipos de acceso.
j) Direcciones y protocolos de la red.
k) Alarmas activadas por el sistema de control de acceso.
l) Activación y desactivación de los sistemas de protección; como sistemas anti-virus y sistemas de detección de intrusiones.

3.7. MANTENIMIENTO DEL PLAN

Periodicidad:

- Cada seis meses
- Cuando se diseñe un nuevo servicio.
- Cambios en los objetivos organizacionales y/o en los procesos del negocio
- Después de un incidente

Responsable: Administrador de la Disponibilidad

Involucrados: Administrador de la Disponibilidad, Gerente General, interesados

3.7.1. MONITORIZACIÓN Y ANÁLISIS DE LAS TENDENCIAS DE GESTIÓN DE LA DISPONIBILIDAD

Las herramientas necesarias para poder realizar un monitoreo más eficiente y que no demandan elevados costos de implementación para la empresa son:

- NAGIOS
- MRTG (*Multi Router Traffic Grapher*)

3.7.2. DETERMINAR LOS REQUISITOS DE DISPONIBILIDAD (Modificados)

Se debe tener en cuenta los siguientes aspectos

Requerimientos:

- Requisitos de disponibilidad del servicio de acuerdo a la necesidad del negocio
- Fallos y criterios de recuperación del servicio
- Elementos de configuración del servicio, son todos los componentes de hardware y software asociados al servicio y que deben estar inventariados.
- Procedimientos de Pruebas de servicios, para identificar componentes defectuosos o dañados

Diseño de la Infraestructura: se debe construir el nuevo diseño de infraestructura en el que se incluyan los nuevos servicios los servicios pueden ser ofrecidos hacia el negocio o para la gestión de TI.

Análisis de Riesgos: identificar los riesgos para los nuevos servicios, en caso de cambios en el servicio e incidentes no considerados.

Diseño de la recuperación: garantizar los componentes del servicio necesarios en caso de fallo de los servicios, para retornar a las operaciones normales del negocio tan rápidamente como sea posible. Tener en cuenta los posibles proveedores y las características del componente.

Consideraciones de Seguridad: Cuando se den cambios en las reglas del negocio.

3.7.3. EL COSTO DE MEJORAR LA DISPONIBILIDAD

Proporcionar información sobre los posibles beneficios y oportunidades de las actualizaciones de tecnológicas previstas que permitan tener mejorar el nivel de disponibilidad establecido.

3.7.4. MÉTODOS Y TÉCNICAS

Los métodos y técnicas que se deben emplear para identificar mejoras son los siguientes:

- CRAMM
- Análisis de Fallos
- El ciclo de vida de incidentes ampliado

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Es esencial que el Diseño de la Disponibilidad esté fuertemente basado en el negocio y en los usuarios, ya que con esto se asegura que la Infraestructura de TI proporcione los niveles de Disponibilidad necesarios para dar soporte a las funciones críticas del negocio, claves para ejecutar sus operaciones.

- El Plan de Disponibilidad de TI para una empresa debe de estar enfocado a mantener la disposición de los servicios de TI para que funcionen ininterrumpidamente, de manera fiable y cumpliendo acuerdos de niveles de servicio de TI para cada actividad del negocio.

- A mayor tiempo de caída de un servicio de TI, mayor será el impacto financiero y operacional en el negocio, por lo que es necesario identificar los procesos críticos del negocio y los servicios relacionados a estos procesos, con los cuales se determinarán los tiempos de recuperación de acuerdo a los niveles de servicios de TI.

- Un Plan de Disponibilidad de TI no sólo se involucra en mantener la disponibilidad de los servicios de TI, sino también en el diseño de la recuperación de estos servicios, para lo cual se toma en cuenta métricas de recuperación, tiempos, costos y efectividad de recuperación de un servicio de TI.

- Aunque se dispongan de las últimas tecnologías y de las herramientas más modernas, es importante tener claro que la disponibilidad de los servicios

de TI no se puede comprar, sino que se la ha de diseñar, implementar, cuantificar y gestionar.

- Si la gestión de la disponibilidad se implementa poniendo un fuerte énfasis en el negocio y los usuarios, se garantiza que la organización considere la disponibilidad como un proceso primordial para que se genere y mantenga un espíritu de mejora continua y una cultura de servicios de TI.

- Aunque en principio todos los clientes estarán de acuerdo con unas elevadas cuotas de disponibilidad, es importante hacerles ver que una alta disponibilidad puede generar unos costos injustificados dadas sus necesidades reales. Quizá unas pocas horas sin un determinado servicio pueden representar poco más allá de una pequeña inconveniencia mientras que la certeza de un servicio prácticamente continuo y sin interrupciones puede requerir la replicación de sistemas u otras medidas igualmente costosas que no van a tener una repercusión real en la rentabilidad del negocio.

4.2. RECOMENDACIONES

- Se recomienda establecer y registrar las mediciones descritas en este proyecto de titulación para todos los incidentes de TI. Esto proporcionará métricas a gestión de la disponibilidad, tanto de los incidentes específicos como de sus tendencias. Los informes regulares sobre la gestión de la disponibilidad, los programas de mejora del servicio y los análisis de caída del sistema pueden hacer uso de esta información y servir de impulso a las actividades de mejora continua en su búsqueda de mejoras efectivas en términos de costos.

- Se recomienda que exista una relación entre la Disponibilidad de los servicios de TI, y las otras disciplinas de la Gestión de servicios de TI, tales como:
    - Gestión de nivel de Servicio

- Gestión de la continuidad de servicio de TI
- Gestión de Relaciones con el Negocio
- Gestión de la Capacidad
- Gestión Financiera de Servicios TI
- Gestión de Aplicaciones
- Las áreas encargadas de la coordinación con los proveedores y de gestionar las relaciones y contratos con ellos.
- Los grupos de soporte técnico encargados de las funciones de pruebas y mantenimiento, en lo referente a la fiabilidad y mantenibilidad de los servicios existentes.

Ya que la relación es bidireccional, la gestión de la disponibilidad proporcionará algunos datos, y al mismo tiempo dependerán de los datos que le suministran las otras disciplinas de la Gestión de servicios de TI.

- Para el Diseño de la Disponibilidad se recomienda poseer una madurez en los procesos de Gestión de Servicio que proporcionen entradas claves para la Gestión de la Disponibilidad, por ejemplo, la Gestión del Nivel de Servicio, la Gestión de la Configuración y la Gestión de Incidentes.

- Se recomienda que cuando se desarrollen nuevos servicios TI, es esencial que la Gestión de la Disponibilidad participe desde el principio, para determinar las necesidades de Disponibilidad; esto influirá en el diseño de la Infraestructura TI, para asegurarse de que se pueda proporcionar el nivel de Disponibilidad necesario.

- Se recomienda mantener el Plan de Disponibilidad actualizado mediante revisiones de cada 6 meses, con el fin de mantener vigente la disponibilidad de los servicios TI.

BIBLIOGRAFÍA

LIBROS Y MANUALES

- Office of Government Commerce (OGC).**Service Delivery**. Crown. U.S.A. 2001
- Office of Government Commerce (OGC). **ITIL la Llave para la Gestión de los Servicios TI**. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007
- Office of Government Commerce (OGC). **ITIL la Llave para la Gestión de los Servicios TI**. Mejores Prácticas para la Provisión del Servicio. versión 3. 2007. Appendix E: Environmental architectures and standards
- Organización Internacional para la Estandarización (ISO), Comisión Electrotécnica Internacional (IEC). **Estándar Internacional ISO/IEC 17799**. 2005
- Syed, Akhtar, Syed, Afsar. **Business Continuity Planning Methodology**. 2004

ARTÍCULOS Y DIRECCIONES ELECTRÓNICAS

- Anónimo. **Administración de Disponibilidad**. http://download.microsoft.com/download/0/B/E/0BE8487E-A38B-4C8F-B796-7CCF1C34CCB4/Nivel2AdministraciondeDisponibilidad.doc. 15-06-2010
- Anónimo. **Análisis del Impacto en el negocio.** http://www.authorstream.com/Presentation/ovalverde-175193-seccion-3-analisis-del-impacto-200903-20090325a-entertainment-ppt-powerpoint/. 01-03-2009
- Camelo, Leonardo. **Análisis de Impacto de Negocios / Business Impact Analysis (BIA).**

http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html, 30-05-2010

- Centro Cristológico Nacional (España), **Objetivo del Punto de Recuperación**, https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/o/rpo.htm. 24-09-2009
- Compute-rs. **Gestión de la Disponibilidad**. http://www.compute-rs.com/es/search.php?search=cramm, 20-06-2010
- IBM. **Plan para la recuperación ante siniestros.** http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzaj1/rzaj1disastr.htm. 20-07-2010
- Kirvan Paul. **IT disaster recovery Plan template**. http://searchdisasterrecovery.techtarget.com/generic/0,295582,sid190_gci1370683,00.html. 13-10-2009
- Osiatis. **Gestión de la Disponibilidad**. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_disponibilidad/proceso_gestion_de_la_disponibilidad/planificacion_de_la_disponibilidad.php. 25-06-2010
- PMG. **Process templates.** http://pmg.net/resources/process-templates. 20-07-2010
- Villalva, Juan. **Riesgos.** http://www.monografias.com/trabajos35/tipos-riesgos/tipos-riesgos.shtml, 20-07-2010
- Wikipedía. **Plan de Recuperación ante desastres**. http://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres, 30-07-2010

TESIS

- Almeida Toapanta Jenny Alexandra. **Análisis de la presentación de servicios apoyados por TI utilizando ITIL en una empresa de servicios públicos.** 2008. Proyecto de Titulación EPN. Quito Febrero 2008

- Amores Vargas Patricia Alexandra. Pachacama Arboleda Gabriela Vanessa. **Implementación de los procesos de service support de ITIL en el área de Tecnología de Grupo Microsistem.** 2007. Proyecto de Titulación ESPE. Sangolquí. Septiembre 2007
- Leiva Garzón Ana Lucia. **Desarrollo del plan de continuidad del negocio para el departamento de TI de una empresa farmacéutica.** 2008. Proyecto de Titulación EPN. Quito Febrero 2008.

ANEXOS

ANEXOS DIGITALES

- **Anexo 1:** Formato para Funciones y Procesos del Negocio
- **Anexo 2:** Sistemas, Aplicaciones y Recursos Críticos de TI
- **Anexo 3:** Tiempos de Recuperación RTO y WRT por Procesos del Negocio
- **Anexo 4:** Objetivo de Punto de Recuperación (RPO) por Procesos del Negocio
- **Anexo 5:** Requerimientos de Disponibilidad
- **Anexo 6:** Análisis por Arboles de Fallo
- **Anexo 7:** Evaluación de Niveles de Riesgo
- **Anexo 8:** Consideraciones de Seguridad - Estándar Internacional ISO/IEC 17799
- **Anexo 9:** Orden de Empastado