ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Ingeniería en Auditoría y Control de Gestión

Plan de Continuidad de Negocios (BCP) para el Área de Sistemas de una empresa dedicada a la manufactura de papel; por el período terminado al 31 de Diciembre del 2008 en la ciudad de Guayaquil.

TESIS DE GRADO

Previo a la obtención del título de:
INGENIERO EN AUDITORÍA Y CONTROL DE GESTIÓN

Especialización:
CALIDAD DE PROCESOS
SISTEMAS INFORMÁTICOS

Presentado por:

Johanna Mariela Sánchez Torbay
Luis Alberto Fierro Fariño

Guayaquil – Ecuador
2008

DEDICATORIA

Este proyecto está dedicado a dios y a nuestros padres, hermanos, familiares y amigos por su apoyo incondicional y por alentarnos día a día.

Sánchez Torbay Johanna Mariela

Fierro Fariño Luis Alberto

AGRADECIMIENTO

Un especial agradecimiento ante todo a nuestro Dios por brindarnos sabiduría y fortalecer la fe, a nuestros maestros que nos ayudaron en nuestra formación académica, a nuestro director de tesis por su apoyo, a la ESPOL por brindarme la oportunidad de forjar nuestros conocimientos y a todas las personas que de una u otra manera colaboraron en la realización de este trabajo.

Sánchez Torbay Johanna Mariela

Fierro Fariño Luis Alberto

TRIBUNAL DE GRADUACIÓN

Ing. Jacqueline Mejía DIRECTOR DE TESIS	Ing. Daltón Noboa DELEGADO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

Luis Fierro Fariño

Johanna Sánchez Torbay

RESUMEN

El presente trabajo abarca la investigación, análisis y proceso que debe contener un plan de continuidad de negocio en caso de contingencia o desastre que afecte a la continuidad de las operaciones de la compañía Clark S.A. La interrupción de las operaciones se pueden dar por diversas causas tales como desastres naturales, humanos, tecnológicos y operacionales esto causa un impacto grave que produciría pérdidas humanas y económicas según la severidad del desastre en caso de no tener implementado un BCP.

Para la realización de nuestro trabajo nos enfocamos en analizar los controles, políticas y procedimientos establecidos por la gerencia para el área de Sistemas IT, el cuál nos permitió planificar nuestro plan. Analizamos las amenazas, vulnerabilidades y riesgos en los procesos de IT. Además se determinó la realización de pruebas de control que permita verificar el correcto funcionamiento del plan, también se estableció el proceso de recuperación de las actividades y un manual de crisis que permita a la compañía enfrentar cualquier tipo de contingencia. Como herramientas de ayuda para nuestro trabajo nos basamos en cuestionarios, tablas, gráficos, check list que sirvan de herramientas de control para evaluar los procesos de IT, así como el análisis de la ejecución del plan. El trabajo presenta nueve capítulos que explica el

contenido del mismo. A continuación detallamos un resumen correspondiente de cada capítulo.

Para el primer capítulo hemos desarrollado el marco teórico que incluye lo más relevante de un plan de continuidad de negocio aplicado a nuestro trabajo, tales como definiciones claves que nos permite entender que es un plan de continuidad y todo el proceso de análisis y ejecución a tener en cuenta.

El segundo capítulo abarca la identificación de la empresa. Para el desarrollo del mismo obtenemos una breve descripción del conocimiento del negocio; analizamos causas, riesgos, probabilidad y vulnerabilidad de los procesos, que conlleven a una interrupción del negocio; identificamos el core business, desarrollamos el análisis de impacto de negocio (BIA) que permita analizar las consecuencias de una ruptura en los componentes del sistema.

Para los demás capítulos identificamos las áreas de trabajo de recuperación, su infraestructura, los datos críticos, vitales, sensitivos y no críticos para luego desarrollar un manual de crisis, esto nos conlleva a realizar el BCP con toda la información recaudada y proceder a hacer pruebas al plan donde se apruebe el correcto funcionamiento del mismo.

Finalmente el resultado de todo esto conlleva a las conclusiones y recomendaciones de nuestro trabajo es decir, determinar si conviene o no realizar un BCP, el impacto que provoca el no implementarlo y lo que debería hacerse para proteger la continuidad del negocio.

TABLA DE CONTENIDO

Pág.

ABREVIATURAS

BCP	Business Continuity Plan
BIA	Business Impact Analysis
SAP	Sistemas, Aplicaciones y Productos
IT	Tecnología de Información
ERP	Planificación de Recursos Empresariales
Ref.	Referencia
Pág.	Página

ÍNDICE DE GRÁFICOS

Pág.

ÍNDICE DE TABLAS

Pág.

INTRODUCCIÓN

Durante las operaciones normales de negocio existe la probabilidad de pérdidas potenciales o interrupciones no programadas asociadas con un desastre o contingencia mayor, por lo que es importante el desarrollo de un plan viable y factible de recuperación que asegure la continuidad de las operaciones de la Compañía.

El planeamiento adecuado, la preparación, y la comunicación son los ingredientes necesarios para un exitoso plan de continuidad de negocio (BCP) en caso de contingencia o desastre.

En el caso de una situación de contingencia o desastre, es importante disponer de una estrategia de recuperación que pueda proveer el reinicio del negocio en un tiempo razonable y predeterminado. Por lo tanto, la importancia de un Plan de contingencias y recuperación en caso de desastres es vital.

El presente documento ilustra los posibles tipos de contingencias y desastres, y los planes de acción para la recuperación de la información y la continuidad del negocio.

La implementación de un Centro de Computo Alterno en el departamento de sistemas permitirá salvaguardar la información y los equipos tecnológicos, que son parte fundamental en la continuidad del negocio.

Este documento contiene un plan estratégico de Sistemas cuyo propósito es asegurar que las inversiones y recursos respecto a tecnología estén en estrecha relación con las estrategias y objetivos del negocio. Además proporciona una dirección estratégica y una estructura común para todas las actividades de ITS con respecto al uso de sus recursos. Asimismo, estas deben cumplir con los estándares corporativos y se deben ceñir a las normas que allí se estipulen.

ALCANCE DEL PROYECTO DE TESIS

El alcance es desarrollar e implementar un Plan de Continuidad de Negocios (BCP) para el Área de Sistemas, el cuál permita mitigar el riesgo de interrupción operacional de vital importancia en caso de algún evento imprevisto, que perjudique la continuidad del negocio.

Además de permitir la pronta recuperación de los sistemas tecnológicos, recuperar las funciones y procesos que requieran la mayor atención posible y proteger los sistemas tecnológicos, recursos y resultados del negocio contra

daños por terceros, daños intencionales o no de los empleados, siniestros naturales y demás causas que pongan en riesgo las actividades de esta área.

JUSTIFICACIÓN DE LA IMPLEMENTACIÓN

Para minimizar el impacto de una contingencia deben existir equipos de repuesto, redes de datos alternas o suministro ininterrumpido de fluido eléctrico. El plan de recuperación en caso de contingencia o desastre considera el disponer de mecanismos para reanudar las actividades de negocio mientras exista dicha contingencia. Mantener y soportar la disponibilidad de las telecomunicaciones se convierte en una actividad vital que asegura la continuidad de las operaciones de negocio de manera normal.

CAPÍTULO I

1. MARCO TEÓRICO

1.1. DEFINICIONES

Plan de Continuidad de Negocio (BCP).- Dado el acaecimiento de tangibles y recientes desastres producidos a nivel mundial, como los efectos del 11 de septiembre del 2001 así como la evolución de la tecnología, este punto de vista ha cambiado, pero no afecta a todos los países y sectores por igual. Del mismo modo, dependiendo del tamaño de la compañía, las acciones varían considerablemente.

British Standards Institution (BSI) En 2007, el BSI publicó la segunda parte, BS 25999-2 "Especificación para Gestión de Continuidad del Negocio", que especifica los requisitos para la aplicación, funcionamiento y mejora de un documentado Sistema de Gestión de la Continuidad del Negocio (BCMS).

Un reciente estudio del Business Continuity Institute del Reino Unido deja claro que los conceptos plan de continuidad de negocio (BCP, Business Continuity Plan) y plan de recuperación de desastres (DRP, Disaster

Recovery Plan) no han sido asimilados adecuadamente por la dirección de las compañías provocando la ineficiencia de sus propios planes.

Un plan de continuidad de negocio (BCP) debe garantizar las operaciones necesarias para cumplir con el funcionamiento establecido en el desarrollo habitual del negocio ante cualquier tipo de desastre, interrupción o contingencia.

Un plan de recuperación de desastres (DRP), por su parte, es el plan que ejecuta Tecnologías de la Información para recuperar los sistemas que gestiona.

Los objetivos de un BCP son minimizar la pérdida financiera de la compañía, continuar con el servicio a los clientes y mitigar los efectos que pueden producirse en los planes estratégicos, la reputación, las operaciones y el mercado donde está situada la compañía.

Según ITIL 2007: (Diseño del Servicio) Plan que define los pasos que se requieren para el Restablecimiento de los Procesos de Negocio después de una interrupción. El Plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, etc. El Plan de la Continuidad del Servicio TI es una parte importante de los Planes de Continuidad del Negocio.

Análisis de Impacto del negocio (BIA).- El propósito del BIA es poner en correlación los componentes específicos del sistema con los servicios críticos que ellos proporcionan, y basado en esa información, para analizar las consecuencias de una ruptura de los componentes del sistema.

El objetivo fundamental es identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre. Además identifica los sistemas críticos y estima el tiempo que la compañía puede tolerar en caso de un desastre.

Un análisis de Impacto de negocio permite abordar un plan de acción con sólidos elementos de criterio basados no sólo en necesidades de capacidad, sino también de seguridad. Para poder definir las contingencias deseadas es necesario conocer los servicios de IT que el departamento de informática ofrece a la compañía, sus vulnerabilidades, así como las amenazas y posibles impactos; además de identificar que servicios de IT soportan los procesos de negocio de la compañía.

Core business.- Es la parte principal de la operaciones del negocio. Es el producto principal del negocio, la razón de venta al cliente.

Contingencia.- Una contingencia se define como cualquier evento no planeado provocando que las actividades de negocio no sean operadas normalmente durante un determinado periodo de tiempo, para la cual existe una solución que permite la recuperación en un tiempo razonable.

Desastre.- Un desastre se define como cualquier evento no planeado que hace un lugar inoperable o inaccesible.

Diversos tipos de desastre pueden ocurrir y varían de comunes, naturales, extraordinarios, etc.

Amenaza.- Es la posible interrupción del negocio a continuar. Son agentes capaces de explotar los fallos de seguridad denominados vulnerabilidades causando pérdidas o daños a los activos.

Vulnerabilidad.- Cualquier debilidad en los sistemas informáticos que puedan ser explotados por las amenazas y causar pérdidas.

Riesgo.- Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático causando un impacto en la empresa.

Backup.- Son copias de seguridad, es el respaldo regular que se da a los sistemas de datos. Los datos podrían respaldarse en discos magnéticos, cintas, discos ópticos (CDs). El método específico escogido para respaldar debe ser basado en los sistemas, disponibilidad de los datos y requisitos de Integridad.

Punto de Recuperación.- El punto de recuperación es en el momento que se puede restablecer todas las operaciones a continuar.

Tiempo de Recuperación.- Es el tiempo que toma recuperar las operaciones continuas del negocio.

CAPÍTULO II

2. IDENTIFICACIÓN DE LA EMPRESA

2.1. CONOCIMIENTO DEL NEGOCIO

2.1.1. Antecedentes de la Empresa

El 3 de febrero de 1995 se constituyó Clark S.A. como compañía en la ciudad de Guayaquil, y tiene como objeto principal la manufactura de papel. El 17 de marzo del mismo año se inicio la comercialización de los productos. Para el mes de junio, se realizaron las primeras ventas de productos en el mercado ecuatoriano.

En su comercialización se han transicionado marcas líderes en marcas corporativas ofreciendo lo último en innovación, tecnología y la más alta calidad en todos los productos.

Diariamente se contribuye a la satisfacción y al bienestar de los consumidores ecuatorianos a través de la difusión de la higiene y la limpieza para bienestar de sus clientes.

CLARK S.A. está conformada por más de 500 empleados y cuenta con un molino en Babahoyo, una planta convertidora en Mapasingue y oficina comercial con bodegas en Quito.

La compañía se fortalece en productos de consumo y uso industrial cada vez más avanzados e inventa otras categorías de productos desechables para la higiene y limpieza personal.

2.1.2. Antecedentes del Área de Sistemas

El Área de Sistemas (IT) proporciona sistemas integrados de información que sirvan como instrumento para la correcta toma de decisiones que le permitan a la compañía ser líder en calidad y sin perder posición competitiva.

Es un área de servicios tanto hacia el interior de la compañía como hacia el entorno externo, por tanto cualquier usuario u otra área que requiera los servicios de IT se convertirán en nuestro cliente al cual se deberá satisfacer respecto a la gestión realizada. Cualquier actividad de IT debe orientarse a resultados que estén de acuerdo con las estrategias y pautas del negocio y que le agreguen valor.

Los usuarios utilizan los sistemas de información existentes como herramientas para gestionar y ejecutar sus actividades, ellos son los que mejor conocen y manejan dichas herramientas. IT es un ente de apoyo y soporte de situaciones “anormales” que no estén contempladas dentro de las operaciones normales.

Toda actividad realizada por el dpto. de IT cumple con las normas corporativas y a su vez deben estar normadas por las políticas de control interno y auditoría. Cualquier situación que atente contra la seguridad o control de la compañía será detectada, registrada y notificada a los niveles directrices de la empresa.

El departamento de IT está compuesto por la siguiente infraestructura: Hardware, Software y Telecomunicaciones las cuáles están correlacionadas para su vital funcionamiento, cuenta con personal especializado que logra un mejor control sobre programas utilitarios, mantenimiento y reparación de equipos, aplicaciones y mantenimiento de la estructura de comunicación que utiliza la compañía.

La misión de ITS es “Proporcionar sistemas integrados de información que sirvan como instrumento para la correcta toma de decisiones que le permitan a la compañía ser líder en calidad y sin perder posición competitiva”.

2.1.3. Misión

Mejorar la salud, higiene y bienestar de las personas cada día y en cada lugar ofreciendo productos de calidad.

2.1.4. Visión

Ser líderes en servicio y costos de distribución, mediante procesos ágiles y eficientes que aseguren el mejor servicio al cliente.

2.1.5. Principales Productos

Los principales productos se clasifican por categoría como: papel higiénico, toallas de mano, servilletas, pañuelos faciales, paños de limpieza, y otros productos.

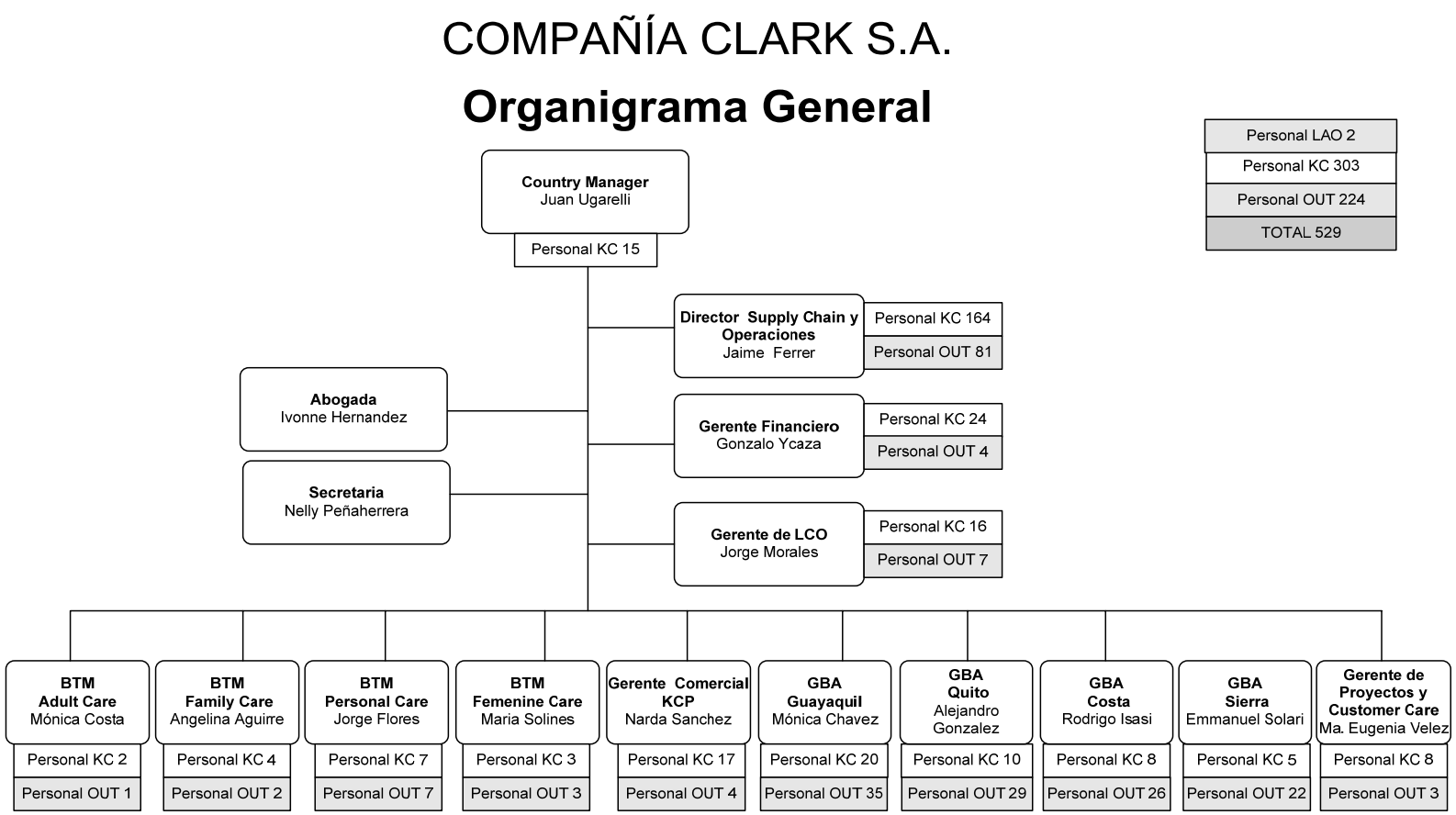
2.1.6. Sectores

- ✓ Sector Oficinas
- ✓ Sector Industrial
- ✓ Sector Salud
- ✓ Sector Hotelería y Turismo
- ✓ Sector Procesadora de Alimentos y Restaurantes
- ✓ Sector Alto Tráfico

2.1.7. Estructura Organizacional

Para el cumplimiento de sus objetivos, la Compañía Clark S.A. cuenta con un personal valioso que contribuye diariamente al buen funcionamiento de la empresa, a brindar un producto de calidad y satisfacción al cliente.

GRÁFICO 2.1: Organigrama General "Clark S.A."



Fuente: Cía. Clark S.A.

2.2. CORE BUSINESS

El Core business de la compañía CLARK S.A. es la fabricación de papel higiénico, debido a que genera la mayor facturación y permanencia en el negocio.

Tabla 2.1 Identificación del Core Business

Ventas Netas – Facturación			
División	**Sector**	**Categoría**	**% Facturación**
01	**Cuidado Familiar**	Papel Higiénico	87%
		Papel Facial	2%
		Tollas domésticas	7%
		Servilletas	4%
	Total Cuidado Familiar 40%		
	Cuidado Infantil y Niños	Papel y Toallas limpiadoras	91%
		Toallas de baño y cuidado corporal	9%
	Total Cuidado Infantil y Niños		**51%**
	Total Cuidado Femenino		**7%**
	Total Cuidado Adultos		**2%**
Total sector 1			**91%**
02	**Nivel Industrial**	Otros productos	2%
		Papel Dispensador de baño	41%
		Papel facial	1%
		Servilletas	8%
		Vestimenta protectora	3%
		Toallas Cuidado de piel	4%
		Toallas Industriales	35%
		Paños limpiadores	7%
	Total Productos Nivel Industrial		**9%**
Total sector 2			**9%**
Total Facturación			**100%**

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.3. ANÁLISIS FINANCIERO

Los costos del proyecto de sistemas, se analizarán mediante un presupuesto anual y serán cargados completamente al área que patrocina el proyecto. Estos costos incluyen infraestructura, personal, telecomunicaciones, compras o arrendamiento de hardware y software, instalaciones y gastos generales. Los costos totales del proyecto deberán ser estimados y firmados para fines de aprobación.

Todos los costos de IT serán detallados por aplicación y función de esta manera nos aseguramos que todos los gastos sean identificados y asignados al correcto centro de costo.

El impacto financiero reduce las ganancias a consecuencia del paro de actividades productivas y generadoras de ingresos. Se detalla el impacto financiero exhaustivo en la tabla 2.20 de la pág 33.

COSTOS:

- ✓ **Infraestructura**

  El valor de la edificación es de $40,000 detallado en la tabla 2.2.

Tabla 2.2: Análisis del Costo de Infraestructura

Edificación	Cantidad	Observación
Aire Acondicionado Central	1	NA
Accesos de seguridad	3	NA
Sensores de Movimiento	4	NA
Sensores de Incendio	6	NA
Fluido de Agua 7x24 (mensual)	1	NA
Servicios Higiénicos M/H	2	NA
Intercomunicadores de Acceso	2	NA

Tabla 2.2: Análisis del Costo de Infraestructura (A continuación)

Edificación	Cantidad	Observación
Extintores (Piso & Oficina)	2	NA
Vigilancia 7x24 (mensual)	8	NA
Alarmas	2	NA
Área oficina		152 m^2

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Costo de Personal**

El Costo de Personal para la administración, seguridad y calidad del servicio es de $32,400 al año, detallado en la siguiente tabla.

Tabla 2.3: Análisis del Costo de Personal

Nº	Cargo	Salario Mensual
1	Coordinador de Sistemas	800
1	Administrador de la Base de Datos	600
1	Administrador de Infraestructura y Servidores.	600
2	Ayudantes de Escritorio (help desk)	350
Total Mensual		**2,700**
Total Anual		**32,400**

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Costo de Telecomunicaciones**

La facturación de telecomunicaciones a través de proveedores externos es de $ 2,468.30 mensual y anual es de $29,619.60.

Tabla 2.4: Análisis del Costo de Telecomunicaciones

COMUNICACIONES	CANTIDAD	OBSERVACION
Switch de comunicaciones	1	NA
Red Inalámbrica	1	Todos los puntos.
Central Telefónica Inalámbrica	1	NA

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Costo de Equipo**

El Costo de Equipo para la implementación necesaria del centro de cómputo es de $6,430 detallado en la siguiente tabla.

Tabla 2.5: Análisis del Costo de Equipo

EQUIPOS	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Estaciones de Trabajo (PIV-512MB-80GB-Wireless Lan)	5	800	4,000
Impresora Matricial	1	250	250
Fax Láser	1	80	80
Impresora Láser	1	600	600
Mobiliario Ejecutivo	5	300	1,500
Total Costo de Equipo			**6,430**

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Gasto de Depreciación de Activos Fijos**

Tabla 2.6: Depreciación de Activos Fijos

Rubro	Valor
Equipos de Computación	4,850
Equipos de Oficina	1,580
Edificación	40,000
Depreciación Eq. Comput. (33.33%)	1,617
Depreciación Eq. Oficina (10%)	158
Depreciación Edificación (5%)	2,000
Total Gasto de Depreciación Anual	3,775

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Gastos Generales y Administrativos**

Tabla 2.7: Gastos Generales y Administrativos

Rubro	Valor Mensual
Agua	300
Luz	500
Teléfono	200
Línea Celular 7x24	30
Costo de Vigilancia 7x24	700
Limpieza y Mantenimiento	120
Gastos administrativos	450
Total Gastos Mensual	**2,300**
Total Gastos Anual	**27,600**

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

BENEFICIO:

Tabla 2.8: Saldos de Ingresos y Costos

Cuentas	Saldos
Ingresos	
Ingresos por Ventas	27,830,320.31
Costos	
Infraestructura	40,000.00
Personal	32,400.00
Telecomunicaciones	29,619.60
Equipo	6,430.00
Gastos de Depreciación	3,775.00
Gastos Generales y Administrativos	27,600.00
Total Costos	139,824.60

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Utilidad o Beneficio Neto = Ingresos – Costos

Utilidad o Beneficio Neto = 27,830,320.31 - 139,824.60

Utilidad o Beneficio Neto = 27,690,495.71

ANALISIS:

- **DESDE EL PUNTO DE VISTA FINANCIERO:**

  El total de Costos es de $139,824.60, el beneficio neto es de $27,830,230.31, por tanto Ingresos menos Costos da un Beneficio de $27,160,495.71 que representa un valor positivo, esto demuestra que existe mayores beneficios al implementar un BCP para la compañía Clark S.A., para lo cual estaremos salvaguardando la información, los equipos y lo más importante la continuidad del negocio. Reduciendo los riesgos que pueden generar pérdidas materiales por daños en los sistemas y equipos, pérdidas humanas en caso de alguna catástrofe y pérdida en la calidad del servicio en caso de interrupciones y daño en la información, esto se daría al no tener implementado un BCP.

- **DESDE EL PUNTO DE VISTA HUMANO:**

  La compañía Clark S.A. cuenta con la cantidad de personal necesaria; capacidad y entrenamiento personalizado; ética y valores admirables; formación académica y habilidades que encajan en el perfil de cada colaborador de la empresa, preparados para cualquier contingencia que pueda ocurrir en la empresa. Además el personal cuenta con conocimientos de:

- ✓ Técnicos de plataforma GD-2000.
- ✓ Básico de SAP.
- ✓ Experiencia con conexión vía RAS.

Tabla 2.9: Análisis del Factor Humano

Factor Humano	Si	No
Capacidad de personal	✓	
Cantidad de personal	✓	
Ética valores del personal	✓	
Formación Académica	✓	

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.4. EVALUACIÓN DEL RIESGO

El propósito de una Valoración del Riesgo es el de conocer los riesgos implicados para las instalaciones de la compañía y el potencial tiempo de caída de las funciones del negocio y operaciones computacionales derivadas. El análisis de estos peligros es muy importante en el desarrollo de un plan de Continuidad del Negocio, el cual es necesario para la recuperación después de una situación de desastre. Los recursos, personal y tiempos necesarios pueden ser identificados después de que el impacto ha sido analizado.

Lo importante es:

1. Entender la vulnerabilidad de que ocurra un desastre y establecer medidas preventivas para eliminar o minimizar la ocurrencia del desastre y;

2. Proveer una localidad segura, no sujeta a los mismos peligros que las instalaciones de computación principales, para respaldar el activo-información en el caso de alguna contingencia.

Para esto listamos las posibles causas de desastre que interrumpan las operaciones:

Tabla 2.10: Posibles Causas de desastre

CAUSAS	DESASTRE
NATURALES	Terremoto Inundación Huracán Nevadas intensas Erupción volcánica Tormentas eléctricas
HUMANAS	Fallas Gerenciales Fallas Directivas Falta de Procedimientos
ECONÓMICAS	Robo Incendio
OPERATIVAS	Fallos masivos Daños accidentales Fallos de energía
TERRORISTAS	Destrucción del centro de cómputo Guerra Atentado Terrorista

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.4.1. Análisis de Probabilidad y Vulnerabilidad

La siguiente tabla clasifica las amenazas potenciales para las instalaciones y el procesamiento computacional por categorías en: amenazas naturales, amenazas humanas y amenazas técnicas.

Cada elemento es calificado ubicando una 'X' en la columna que mejor califica la vulnerabilidad a la amenaza. La escala es de 1 hasta 10, donde 1 indica un bajo riesgo de exposición, a partir del valor 5 indicaría la necesidad de atención, a fin de asegurar que se establezcan medidas preventivas, en donde sea aplicable, y además de que el respaldo de la información sea seguro.

Es importante entender que esta evaluación es subjetiva y su intención es ayudar a las instalaciones en la protección y respaldo de información y registros vitales de la compañía.

Tabla 2.11: Análisis de Probabilidad y Vulnerabilidad

Categoría	[En escala de 1-a-10, donde 1 indica baja vulnerabilidad] baja…….....alta									
Amenazas Naturales:	1	2	3	4	5	6	7	8	9	10
Inundaciones internas	X									
Inundaciones Externas			X							
Fuego interno		X								
Fuego Externo					X					
Terremoto	X									
Volcanes	X									
Huracanes	X									
Tornado	X									
Rayos	X									
Nevadas	X									
Avalancha	X									
Amenazas Humanas :										
Explosión	X									
Vandalismo			X							
Robo		X								
Obstrucción para ir al trabajo		X								
Deshechos tóxicos	X									
Caídas de aviones	X									
Accidentes	X									
Terrorismo	X									
Amenazas Técnicas:										
Fallos de energía						X				
Comunicaciones de datos			X							
Fallos del aire acondicionado			X							
Fallos del CPU y Hardware					X					
Fallos del Software del sistema			X							
Fallos del Software aplicativo					X					
Interferencia Electromagnético			X							
Otro	X									

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.5. ANÁLISIS DEL RIESGO

El siguiente cuadro se resume el análisis de probabilidad y vulnerabilidad con los riesgos detectados para cada caso.

Tabla 2.12:Probabilidad, Vulnerabilidad y Riesgos Detectados

Posibles Amenazas	Probabilidad (%)				Vulnerabilidad ($)				Riesgos Detectados
	A	M	B	NA	A	M	B	NA	
Naturales:									
Inundaciones			x			X			Vidas humanas y pérdidas económicas. Paralización de actividades.
Sismos		x					x		Vidas humanas y pérdidas económicas. Paralización de actividades.
Tormenta eléctrica		x					x		Sistemas de redes colapsados.
Humanas:									
Fallas gerenciales			x			x			Daño en los sistemas y equipos.
Fallas directivas			x			x			Daño en los sistemas y equipos.
Falta de Procedimientos			x			x			Daño en los sistemas y equipos.
Económicas:									
Incendios		x					x		Vidas humanas y pérdidas económicas. Paralización de actividades.
Robos		x					x		Pérdidas económicas
Sabotaje Computacional			x			x			Daño en los sistemas, equipos y pérdidas económicas.
Operativos:									
Fallos masivos			x			x			Sistema colapsado.
Daños accidentales			x			x			Daño en los sistemas y equipos.
Marcha, mítines, etc.				x	x				Pérdidas económicas. Paralización de actividades.
Terroristas:									
Destrucción del Centro de Cómputo			x			x			Vidas humanas y pérdidas económicas. Paralización de actividades.
Guerra				x	x				Vidas humanas y pérdidas económicas. Paralización de actividades.
Atentado terrorista				x	x				Vidas humanas y pérdidas económicas. Paralización de actividades.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Leyenda:

A = Alta M = Media B = Baja NA = Ninguna

Ley inversa:

Mayor Probabilidad ➔ Menor Vulnerabilidad

Menor Probabilidad ➔ Mayor Vulnerabilidad

2.6. ANÁLISIS DE CRITICIDAD

2.6.1. Clasificación de las Operaciones

Tabla 2.13: Análisis de Criticidad de las Operaciones

Operaciones	Posibles Causas
CRÍTICAS	Falla de la red en una localidad.
	Falla de los enlaces de telecomunicaciones entre localidades.
	Falla del servidor de aplicaciones.
	Falta de suministro eléctrico.
VITALES	Fallas humanas en la operación de la red.
	Fallas humanas en la operación de los equipos de cómputo.
	Fallas humanas en el mantenimiento de redes y equipos.
SENSITIVAS	Cambio climático (Estacionalidad).
	Clientes.
NO CRÍTICAS	Cambios de departamentalización indirecta.
	Errores no críticos del usuario.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.7. CUANTIFICACION DEL PUNTO Y TIEMPO DE RECUPERACIÓN

2.7.1. Análisis del Punto de Recuperación

El punto de recuperación se lo realiza en la mayor brevedad posible, donde se minimice el tiempo de afectación del paro de actividades. Para el análisis del punto de recuperación tomamos en cuenta los siguientes parámetros:

- ✓ **Capacidad** (experiencia)**:** Cuenta con el personal adecuado y capacitado con conocimientos básicos especialmente en plataforma GD-2000, SAP y conexión vía RAS que es lo esencial para la administración de una contingencia.

- ✓ **Financiero:** Hemos demostrado mediante un análisis financiero (hacer referencia de la pág 12 – 16) que mayor es el beneficio que el costo de recuperación.

- ✓ **Ubicación geográfica:** La ubicación de nuestro centro de cómputo alterno es en la ciudad de Babahoyo, este sitio es propio de la compañía. Este se encuentra por lo menos a 70 Km. de la matriz (Guayaquil), la localidad está en una zona plana y segura, cuenta con todos los servicios disponibles en caso de una contingencia.

2.7.2. Análisis del Tiempo de Recuperación

El análisis del tiempo de recuperación depende de los siguientes parámetros:

- ✓ **Capacidad:** Medimos la capacidad del personal anteriormente. Podemos decir que el personal está completamente capacitado en caso de contingencia.

- ✓ **Ubicación geográfica:** Analizamos la ubicación geográfica y resulta que está en muy buena zona con todos los servicios disponibles a su alrededor y se encuentra alejada de la matriz.

Tabla 2.14: Análisis del tiempo de recuperación

Parámetros	Alta	Mediana	Baja
Capacidad (experiencia)	✓		
Ubicación geográfica	✓		

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

La instalación de 1 PC tarda aproximadamente 1 hora 20 minutos instalarlos, para el resto de los equipos se tardará aproximadamente entre 10 a 15 minutos, instalaciones de programas 2 horas. Tiempo total de instalación de las 5 estaciones es de 4 horas.

2.8. ANÁLISIS DEL IMPACTO DEL NEGOCIO (BIA)

2.8.1. Desarrollo del BIA

2.8.1.1. Propósito del BIA

El propósito del BIA es disponer de una estrategia de recuperación que pueda proveer el reinicio del negocio en un tiempo razonable y predeterminado en caso de una contingencia.

2.8.1.2. Objetivos del BIA

Los objetivos del plan de recuperación en caso de desastre son los siguientes:

- Minimizar los efectos de una contingencia o desastre en las funciones críticas al proveer de un conjunto de procedimientos y tareas a ser usados en el evento.

- Responder a una situación de contingencia o desastre rápida y efectivamente.

- Reunir al personal necesario para reactivar el proceso con las interrupciones menores respecto al servicio al cliente.

- Restauración por fases en el tiempo de todas las aplicaciones y servicios posteriormente a la interrupción a causa de la contingencia o desastre.

Este plan busca minimizar:

- El número de decisiones que deben ser hechas después de una contingencia o desastre.
- La necesidad de desarrollar, probar, y corregir nuevos procedimientos durante el desastre.
- Depender de la participación de cualquier persona específica o grupo de personas durante el proceso de recuperación.
- El período de tiempo tomado para el proceso de recuperación.
- Las pérdidas asociadas con la interrupción de las actividades del negocio.
- La confusión y la exposición a errores.
- La duplicación de esfuerzos.

El alcance de estos objetivos asegurará la estabilidad operacional a través de un proceso de recuperación.

2.8.1.3. Alcance

Este plan es exclusivamente para las operaciones del área de Sistemas de la compañía Clark S.A. No documenta las acciones específicas de los departamentos del negocio o una estrategia de recuperación global corporativa.

El plan considera los siguientes aspectos:

- Reestablecimiento de los equipos y enlaces de telecomunicaciones vitales para la operación del negocio.

- Reestablecimiento de las áreas vitales de la red de computadoras.

El plan no considera los siguientes aspectos:

1. Emergencias de edificios y procedimientos de evacuación.
2. Valoración de riesgos en los edificios.

3. Evaluación y declaración de desastres en edificios.
4. Recuperación de las diferentes unidades y departamentos de la Compañía.
5. Equipos no relacionados con la red de datos (PBX, máquinas de fax, fotocopiadoras, etc.)

2.8.1.4. Suposiciones, sucesos y tiempo

1. Falla de la red.
2. Falla en los enlaces de telecomunicaciones.
3. Falta de suministro de corriente eléctrica.
4. Fallas humanas en la operación de la red o equipos de cómputo.

El presente plan de contingencias y recuperación en caso de desastre considerará los siguientes desastres:

- Tormentas eléctricas que destruyan parcial o totalmente la red de datos.
- Fallas físicas en la red de datos y o comunicaciones.

2.8.1.4.1. Procedimiento para atención de fallas

- ✓ **Conexión física a la red local**

Tabla 2.15: Análisis de la Conexión Física

Problema:	No hay acceso a la red de datos.
Acción:	1. Determinar si el usuario está conectado a la red. 2. Corregir problemas de nivel físico, conectores, LAN Jack, Switch. 3. Si se determina que el problema es una avería que va a ser resuelta por más de 6 horas, habilitar puntos de red de emergencia.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Acceso al Enterprise Network**

Tabla 2.16: Análisis del Enterprise Network

Problema:	No hay acceso al Global Desktop.
Acción:	1. Revisar entorno de red. 2. Si no hay acceso al GDXP, reportar enlace al proveedor local. 3. Si la falla y/o resolución del problema se demora más de 6 horas comunicar a usuarios claves el acceso alternativo vía RAS 4. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Acceso al File&Print Server**

Tabla 2.17: Análisis de las Impresoras

Problema:	Problema no se puede imprimir o acceder archivos en el servidor.
Acción:	1. Revisar acceso tipo share. 2. Revisar si puede imprimir desde Windows. 3. Revisar los servicios del servidor. 4. Contactar a "Help-Desk" MIS Local. 5. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Acceso al Correo Electrónico**

Tabla 2.18: Análisis de Acceso al e-mail

Problema:	No hay acceso al correo electrónico.
Acción:	1. Revisar si hay acceso al Address Book. 2. Enviar y/o recibir correo. 3. Si no se pueden realizar las acciones anteriores, contactar al Help Desk de MIS Local. 4. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.8.1.5. Identificación de las funciones y procesos del Negocio

El objetivo principal de este paso es identificar los procesos y funciones que son soportes de la compañía, la cuál conlleva a cumplir con la meta corporativa.

Tabla 2.19: Funciones y procesos del negocio

Funciones	Procesos
Hardware	Mantenimiento de Equipos
	Instalación de Equipos
	Help desk
	Soporte a los departamentos
Software	Instalación de Programas
	Configuración de Equipos
	Encriptación de la Información Sensitiva.
	Acreditación de Programas
	Administración de datos
	Seguridad de la información.
	Respaldo de la Información (Backup).
Telecomunicaciones	Configuración y Mantenimiento de redes
	Mantenimiento de equipos de comunicación
	Monitoreo de la red.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.8.1.6. Valoración del Impacto Financiero y Operacional

La Valoración del Impacto financiero y operacional es conocer lo que los riesgos y pérdidas económicas implican para los procesos de la compañía y el potencial tiempo de caída de las funciones del negocio.

A continuación clasificamos el rango del impacto según el nivel de severidad de 0 a 3, donde 0 no existe impacto y tres produce mayor impacto, basado en la pérdida financiera por día.

Escala de Niveles de Severidad:

1. Nivel de severidad 0 ➔ No genera Impacto
2. Nivel de severidad 1 ➔ Menor Impacto
3. Nivel de severidad 2 ➔ Mediano Impacto
4. Nivel de severidad 3 ➔ Mayor Impacto

Tabla 2.20: Impacto Financiero

Funciones	Procesos	Pérdida Financiera por día ($)	Nivel de Severidad
Hardware	Mantenimiento de Equipos	Media	2
	Instalación de Equipos	Baja	1
	Help desk	Media	2
	Soporte a los departamentos	Alta	3
Software	Instalación de Programas	Baja	1
	Configuración de Equipos	Media	2
	Encriptación de la Información Sensitiva.	Alta	3
	Acreditación de Programas	Baja	1
	Administración de datos	Media	2
	Seguridad de la información.	Alta	3
	Respaldo de la Información (Backup).	Alta	3
Telecomunicaciones	Configuración y Mantenimiento de redes	Media	2
	Mantenimiento de equipos de comunicación	Media	2
	Monitoreo de la red.	Alta	3

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Tabla 2.21: Impacto Operacional

Funciones	Procesos	Nivel de Impacto Operacional			
		A	M	B	N/A
Hardware	Mantenimiento de Equipos	**X**			
	Instalación de Equipos			**X**	
	Help desk	**X**			
	Soporte a los departamentos	**X**			
Software	Instalación de Programas			**X**	
	Configuración de Equipos		**X**		
	Encriptación de la Información Sensitiva.	**X**			
	Acreditación de Programas				**X**
	Administración de datos	**X**			
	Seguridad de la información.	**X**			
	Respaldo de la Información (Backup).	**X**			
Telecomunicaciones	Configuración y Mantenimiento de redes		**X**		
	Mantenimiento de equipos de comunicación	**X**			
	Monitoreo de la red.	**X**			

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Leyenda:

A = Alta M = Media B = Baja NA = Ninguna

2.8.1.7. Identificación de Procesos Críticos

En esta sección analizamos la criticidad de los procesos de cada función del área de IT, lo cuál detallamos en la tabla 1.18:

Tabla 2.22: Procesos Críticos

Funciones	Procesos	Criticidad
Hardware	Mantenimiento de Equipos	Vitales
	Instalación de Equipos	Vitales
	Help desk	Sensitiva
	Soporte a los departamentos	Crítica
Software	Instalación de Programas	Vitales
	Configuración de Equipos	Crítica
	Encriptación de la Información Sensitiva.	Crítica
	Acreditación de Programas	Sensitiva
	Administración de datos	Crítica
	Seguridad de la información.	Crítica
	Respaldo de la Información (Backup).	Crítica
Telecomunicaciones	Configuración y Mantenimiento de redes	Vitales
	Mantenimiento de equipos de comunicación	Vitales
	Monitoreo de la red.	Sensitiva

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Activos de Información

La Administración de ITS responsable por las Instalaciones Computacionales, está conciente de la importancia de asegurar los registros vitales y el respaldo de la información residente en las computadoras. Esta información necesita estar almacenada en una localidad que no esté sujeta a las mismas amenazas de las instalaciones principales.

La pérdida de estos respaldos al mismo tiempo de un desastre, dejaría a la compañía en una situación vulnerable.

2.8.1.8. Identificación MTDs y Priorización de los Procesos Críticos

En esta sección identificamos el tiempo máximo tolerable de recuperación de los procesos de cada función del área de IT, para la cuál detallamos en la siguiente tabla el tiempo y prioridad de recuperación para la continuidad de las operaciones diarias.

Tabla 2.23: Máximo tiempo tolerable de Recuperación (MTDS)

Funciones	Procesos	MTD	Prioridad de Recuperación
Hardware	Mantenimiento de Equipos	1 día	Baja
	Instalación de Equipos	1 día	Alta
	Help desk	1 día	Baja
	Soporte a los departamentos	1 día	Alta
Software	Instalación de Programas	1 día	Alta
	Configuración de Equipos	1 día	Alta
	Encriptación de la Información Sensitiva.	1 día	Alta
	Acreditación de Programas	1 día	Baja
	Administración de datos	1 día	Alta
	Seguridad de la información.	1 día	Alta
	Respaldo de la Información (Backup).	1 día	Alta
Telecomunicaciones	Configuración y Mantenimiento de redes	2 días	Alta
	Mantenimiento de equipos de comunicación	1 día	Media
	Monitoreo de la red.	1 día	Media

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.8.1.9. Identificación de los Procesos Críticos de IT. Sistemas y Aplicaciones

Tabla 2.24: Procesos Críticos de IT

Funciones	Procesos	Criticidad de los Sistemas y Aplicaciones de IT
Hardware	Mantenimiento de Equipos	ERP
	Instalación de Equipos	ERP
	Help desk	Customer Relationship Management (CRM)
	Soporte a los departamentos	Customer Relationship Management (CRM) Order to cash Forecast to stock Requisition to payment Accounting to reporting
Software	Instalación de Programas	Management (CRM) Order to cash Forecast to stock Requisition to payment Accounting to reporting
	Configuración de Equipos	Customer Relationship Management (CRM) Order to cash
	Encriptación de la Información Sensitiva.	Accounting to reporting
	Acreditación de Programas	Customer Relationship Management (CRM)
	Administración de datos	Order to cash Forecast to stock Requisition to payment
	Seguridad de la información.	Customer Relationship Management (CRM)
	Respaldo de la Información (Backup).	Management (CRM) Order to cash Forecast to stock Requisition to payment Accounting to reporting

Tabla 2.24: Procesos Críticos de IT (Continuación)

Funciones	Procesos	Criticidad de los Sistemas y Aplicaciones de IT
Telecomunicaciones	Configuración y Mantenimiento de redes	ERP
	Mantenimiento de equipos de comunicación	ERP
	Monitoreo de la red.	ERP

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

2.8.1.10. Recursos Críticos de No IT

Los recursos críticos que no son propiamente de tecnología de información, son los siguientes:

- Muebles y enseres
- Edificación
- Equipos de oficina
- Útiles de Oficina y papelería
- Materia Prima
- Materiales de uso y consumo
- Producto Final
- Equipos de seguridad
- Equipos de comunicación de voz
- Registros y manuales críticos
- Maquinarias
- Herramientas de trabajo y mantenimiento

2.8.1.11. Determinación del Objetivo de tiempo de Recuperación (RTO)

El objetivo principal es de salvaguardar la información y los equipos, para lo cuál se establece una política de generar backup automáticamente al término de cada jornada, además de brindar seguridad a los equipos a través de pólizas de seguridad, esto permite minimizar el impacto.

Además el mayor tiempo que se establecería es de 48 horas para poder generar backup de la información crítica y relevante de la compañía. El tiempo de recuperación de las operaciones del negocio se dará según la intensidad del desastre.

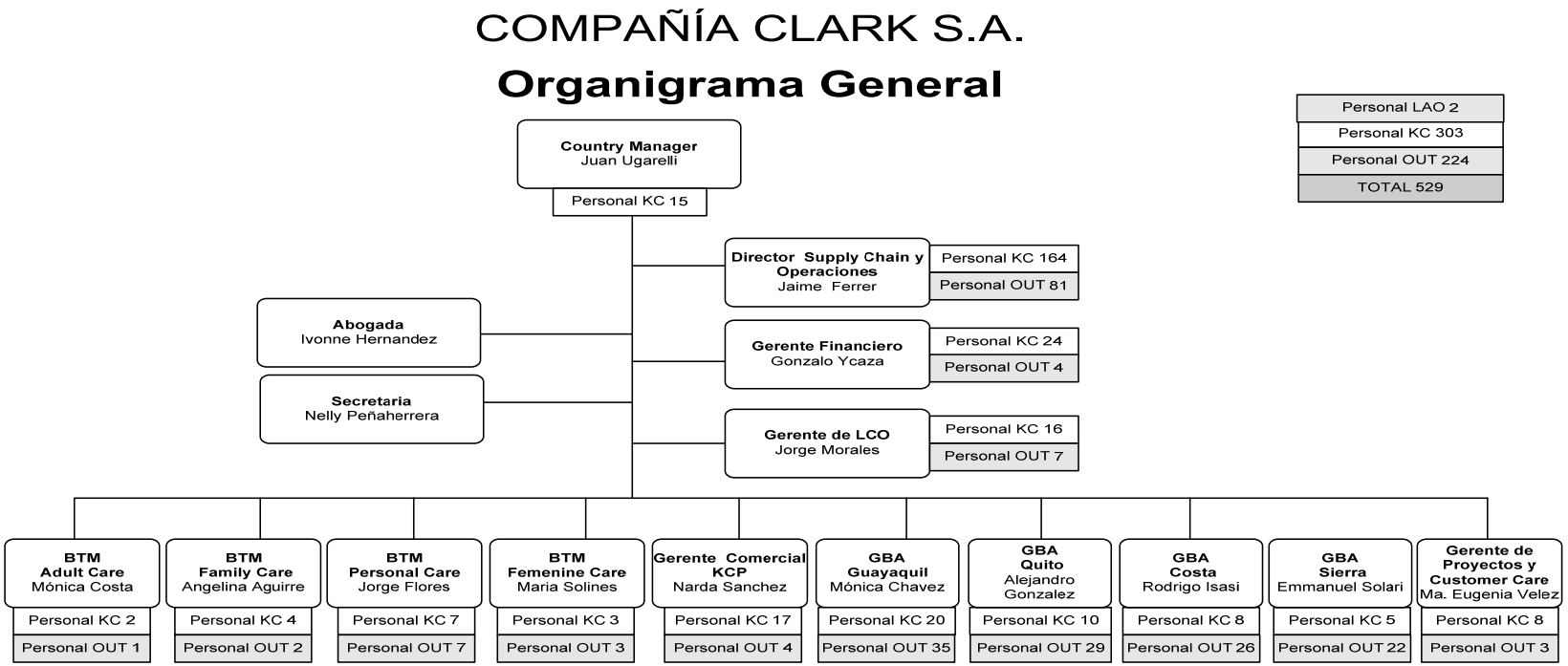
2.8.1.12. Identificación del Procedimiento de la Continuidad del Negocio

- Manual de Administración de Crisis
- Manual de Recuperación en caso de desastre
- Manual de Operaciones
- Manual de reanudación de nóminas y cubos de información.
- Políticas y Procedimientos alternos en caso de emergencia.

CAPÍTULO III

3. IDENTIFICACIÓN DEL ÁREA DE TRABAJO DE RECUPERACIÓN

3.1. ESTRUCTURA ORGANIZACIONAL GENERAL



3.1.1. Descripción de los Perfiles y Responsabilidades del Organigrama General

- **Gerente General:**

Misión del Cargo: Planear, coordinar y controlar las estrategias, actividades, cultura y procesos del negocio con el fin de garantizar el cumplimiento de los objetivos de la operación de la compañía Clark S.A., siguiendo las políticas corporativas.

Relaciones de Trabajo:

Relaciones Internas				
Área	**N**	**B**	**I**	**C**
Finanzas				X
Mercadeo				X
LCO				X
Gerencia				
Supply				X
Ventas				X
Operaciones				X

Relaciones Externas				
Entes	**N**	**B**	**I**	**C**
Proveedores			X	
Clientes				X
Consumidores				X
Entes Gubernamentales			X	
Asociaciones		X		
Otros			X	

N: Ninguna B: Básica I: Importante C: Crítica

Responsabilidad y Funciones:

- Diseñar las actividades comerciales y los planes de desarrollo para los diferentes clientes, así como asesorar su implementación con el fin de cumplir con los objetivos de venta y rentabilidad establecidos. Programar implementaciones tecnológicas definidas por la corporación para mejorar y mantener la operación.
- Asesorar la elaboración de los planes de mercadeo y su aprobación final, buscando alcanzar los objetivos de venta y de participación de mercado establecidos.
- Establecer en conjunto con Recursos Humanos los planes y acciones de Gestión humana, con el fin de asegurar la calidad, motivación, capacitación y crecimiento del personal que contribuya en forma eficaz al cumplimiento de los objetivos de la compañía y que garanticen la cultura corporativa.
- Coordinar y hacer seguimiento a iniciativas en los procesos de la Cadena de Abastecimiento y Operaciones, así como proponer acciones de mejora con el fin de garantizar la disponibilidad oportuna y el costo necesario de los productos para soportar el área comercial.

- Establecer los presupuestos totales y por categoría de producto así como asesorar en su ejecución con el fin de asegurar que los resultados se cumplan y que los mismos respondan con la rentabilidad definida.

- Asesorar y supervisar la ejecución los planes de responsabilidad social así como coordinar su implementación, buscando promover acciones sociales que generen un vínculo con la sociedad.

- Hacer seguimiento a la implementación de las políticas y controles definidos por la corporación buscando asegurar que todas las áreas cumplan con los estándares definidos.

- Dirigir, coordinar y controlar el presupuesto, los planes y programas de control interno que garanticen la sustentabilidad de los resultados financieros acorde con los CFI corporativos y las leyes locales.

Autoridad – Recomienda y Decide:

Decisiones	Recomendaciones
Política y estrategia comercial Planes de mercadeo Presupuestos Contratación y despido de personal Incremento salarial Políticas y planes de Recursos Humanos Acciones de la cadena de abastecimiento Actividades de Responsabilidad Social	Política salarial Despidos de personal de primer nivel Cambios en la definición de productos Cambios de estructura

Educación: Profesional

Conocimientos: Inglés (Alto), Conocimiento en mercadeo, ventas.

Experiencia: 5 años, Gerencia Funcional (Mercadeo o Ventas).

Habilidades: Capacidad trabajo bajo presión, Trabajo en equipo, Trabajo individual, Responsabilidad, Interacción y comunicación social, Liderazgo, Orientación a resultados.

- **Gerente Financiero:**

Misión del Cargo: Administrar eficientemente el otorgamiento y gestión del crédito a nivel nacional y asegurar la recuperación de la cartera de clientes para contribuir a un crecimiento sostenible del negocio.

Relaciones de Trabajo:

Relaciones Internas				
Área	**N**	**B**	**I**	**C**
Finanzas				X
Mercadeo		X		
LCO		X		
Gerencia			X	
Supply				X
Ventas				X
Operaciones	X			

Relaciones Externas				
Entes	**N**	**B**	**I**	**C**
Proveedores			X	
Clientes				X
Consumidores	X			
Entes Gubernamentales	X			
Asociaciones	X			
Otros	X			

N: Ninguna B: Básica I: Importante C: Crítica

Responsabilidad y Funciones:

- Administrar del portafolio de clientes a nivel nacional, lo cual se relaciona con crear vínculos importantes con el cliente y su estructura que brinde un mayor poder de negociación a fin de mejorar la rotación de cartera de la cía.

- Coordinar con el área comercial la recuperación y administración eficiente de cartera, que contribuya a la mejora de los indicadores y nos permita minimizar riesgos de cartera.
- Aprobar pedidos y días de crédito de clientes para contribuir con la negociación comercial del equipo de ventas con el cliente.
- Garantizar el flujo de efectivo de la compañía implicando una cobranza a tiempo para lograr un exacto cumplimiento de las obligaciones contraídas por KCE.
- Desarrollar proyectos acorde a las necesidades del negocio para mejorar los índices de recuperación de cartera.
- Revisar y aprobar solicitudes de clientes potenciales y aumentos de cupos de clientes importantes de cada zona en KCE para incrementar las cuotas de ventas con cada uno de ellos.
- Gestionar garantías reales de clientes minimizando el riesgo de cuentas incobrables para asegurar un crecimiento sostenible del negocio.
- Liquidar comisiones de cobranzas del equipo comercial para incentivar mejora en su gestión de cobranza.

- Aprobar liquidaciones de rebates de clientes condicionados al pago a tiempo de sus facturas, para incentivar al cliente por haber cumplido con su cuota de venta y pagos.
- Reportar, investigar y manejar de manera puntual actos y condiciones deficientes e identificar aspectos y riesgos llevándolos a niveles aceptables de riesgo o impacto para garantizar que sea una Planta de Clase Mundial.

Autoridad – Recomienda y Decide:

Decisiones	Recomendaciones
Negociación con clientes Aprobación de facturación	Recomendación de cupos de clientes nuevos > a $50,000.00 o excesos de cupo de clientes existentes > al 150%.

Educación: Maestría en Administración de Empresas o afines. Titulo Universitario en Ing. Comercial, Finanzas, Gestión Empresarial.

Conocimientos: Ingles intermedio conversacional. Dominio de herramientas office, Excel avanzado.

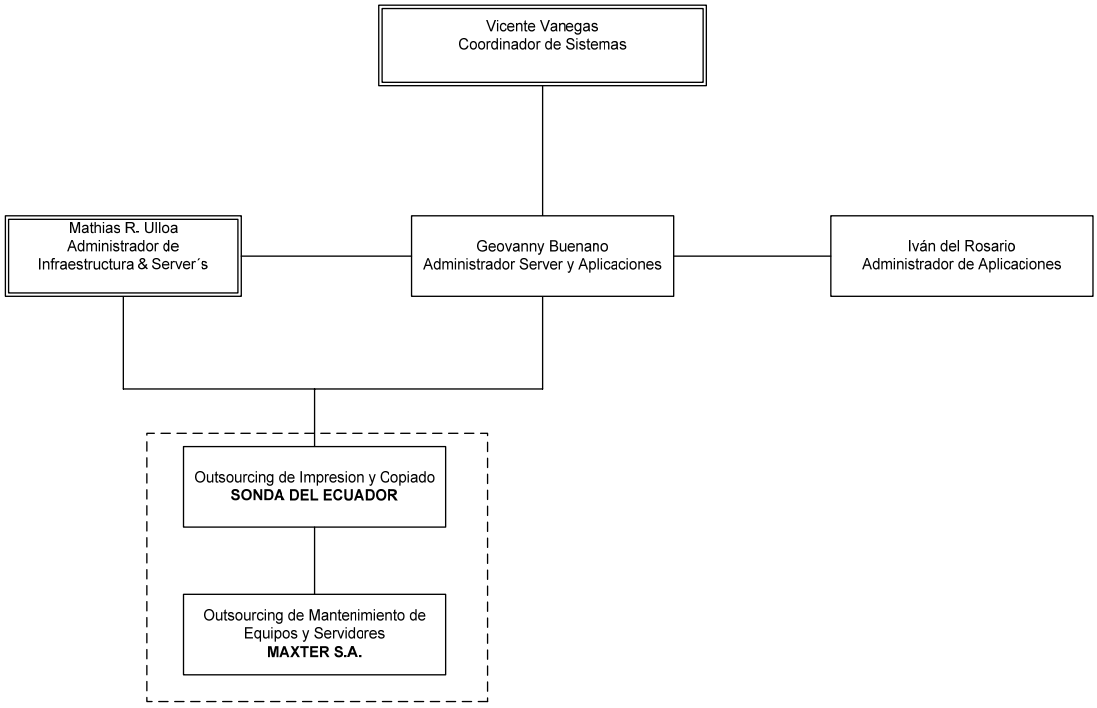
Experiencia: 2 años en cargos similares y/o afines.

Habilidades: Capacidad de trabajo bajo presión, habilidad numérica, negociación, trabajo en equipo, responsabilidad, interacción y comunicación social, liderazgo y orientación a resultados.

3.2. ESTRUCTURA ORGANIZACIONAL DEL ÁREA IT

Gráfico 3.1: Estructura Organizacional de IT

COMPAÑÍA CLARK S.A.
Organigrama Departamental
M.I.S.



Fuente: Cía. Clark S.A.

3.2.1. Descripción de los Perfiles y Responsabilidades del Área de IT

- **Coordinador de ITS:**

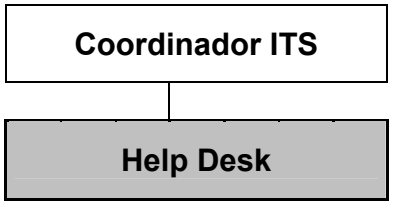
Misión del Cargo: Administrar y controlar proyectos y recursos tecnológicos siguiendo las políticas y estándares de la corporación para asegurar y mejorar la operación del negocio.

Relaciones de Trabajo:

Relaciones Internas				
Área	**N**	**B**	**I**	**C**
Finanzas			X	
Mercadeo			X	
LCO			X	
Gerencia			X	
Supply				X
Ventas			X	
Operaciones				X

Relaciones Externas				
Entes	**N**	**B**	**I**	**C**
Proveedores		X		
Clientes	X			
Consumidores	X			
Entes Gubernamentales	X			
Asociaciones	X			
Otros	X			

N: Ninguna B: Básica I: Importante C: Crítica



Responsabilidad y Funciones:

- Programar planes de mantenimiento de infraestructura (RED, Servidores, Comunicaciones) y aplicaciones para mantener funcionamiento de los mismos.
- Programar implementaciones tecnológicas definidas por la corporación para mejorar y mantener la operación.
- Supervisar el apropiado desenvolvimiento de las operaciones dentro del área, con la finalidad de garantizar el fiel cumplimiento de los controles internos & SOX.
- Supervisión de servicios tercerizados para garantizar la normal operación del negocio.
- Supervisar las actividades de desarrollo e infraestructura para lograr eficiencia en los procesos.
- Programar los planes de contingencia sobre servidores y acceso a red con la finalidad de mantener operativo el negocio.
- Programar nuevo requerimiento de usuario o necesidades internas de información para mejorar la gestión y la toma decisión.
- Reportar, investigar y manejar de manera puntual actos y condiciones deficientes e identificar aspectos y riesgos

llevándolos a niveles aceptables de riesgo o impacto para garantizar que sea una Planta de Clase Mundial.

Autoridad – Recomienda y Decide:

- Decisiones de tipo técnicas.
- Recomendaciones de tipo tecnológicas.

Educación: Ingeniero de sistemas y/o analista de sistemas.

Conocimiento: Telecomunicaciones (CISCO), base de datos SQL, servidores Windows 2003.

Experiencia: 4 a 5 años en cargos similares.

Habilidades: Capacidad trabajo bajo presión, trabajo en equipo, trabajo individual, responsabilidad, interacción y comunicación social, liderazgo, orientación a resultados.

- **Help desk:**

Misión del Cargo: Verificar y corregir los problemas de hardware y software brindando una excelente atención técnica a los usuarios internos, aplicando las mejores prácticas en el manejo de herramientas para garantizar el buen funcionamiento de todas las herramientas tecnológicas de la compañía.

Relaciones de Trabajo:

Relaciones Internas				
Área	**N**	**B**	**I**	**C**
Finanzas				X
Mercadeo				X
LCO				X
Gerencia General				X
Supply				X
Ventas				X
Operaciones				X

Relaciones Externas				
Entes	**N**	**B**	**I**	**C**
Proveedores		X		
Clientes	X			
Consumidores	X			
Entes Gubernamentales	X			
Asociaciones	X			
Otros	X			

N: Ninguna B: Básica I: Importante C: Crítica

Responsabilidades:

- Monitorear y garantizar el correcto funcionamiento de los equipos de comunicación de la compañía para asegurar la continuidad del negocio.

- Ejecutar los planes de contingencia sobre servidores y equipos de comunicación, según los procedimientos establecidos para garantizar la continuidad del negocio.

- Ejecutar los trabajos de mantenimiento en los servidores y/o equipos de comunicación para garantizar la continuidad del negocio.

- Brindar soporte a los usuarios en temas relacionados al acceso de la información, hardware y software para contribuir a su buen desempeño laboral.

- Controlar el correcto y adecuado uso de las herramientas de comunicación telefónicas para asegurar su correcto funcionamiento.

- Documentar los procesos del área a través de procedimientos escritos, formatos y registros, a fin de cumplir con la política de control interno & SOX y minimizar los riesgos de contingencias.

- Garantizar el adecuado funcionamiento del cableado de red de cada localidad de la compañía manteniendo el estándar de la corporación para favorecer al correcto funcionamiento y operatibilidad del negocio.

- Reportar e investigar de manera puntual actos y condiciones deficientes y operar las áreas de trabajo e instalaciones en total cumplimiento con las leyes y códigos locales para asegurar que la Planta funcione bajo los estándares establecidos.

Autoridad – Recomienda y Decide:

- Decisiones N/A.
- Recomendaciones al usuario final para mejores prácticas en el manejo de las herramientas tecnológicas.

Educación: Técnico Superior en Sistemas, Analista de Sistemas.

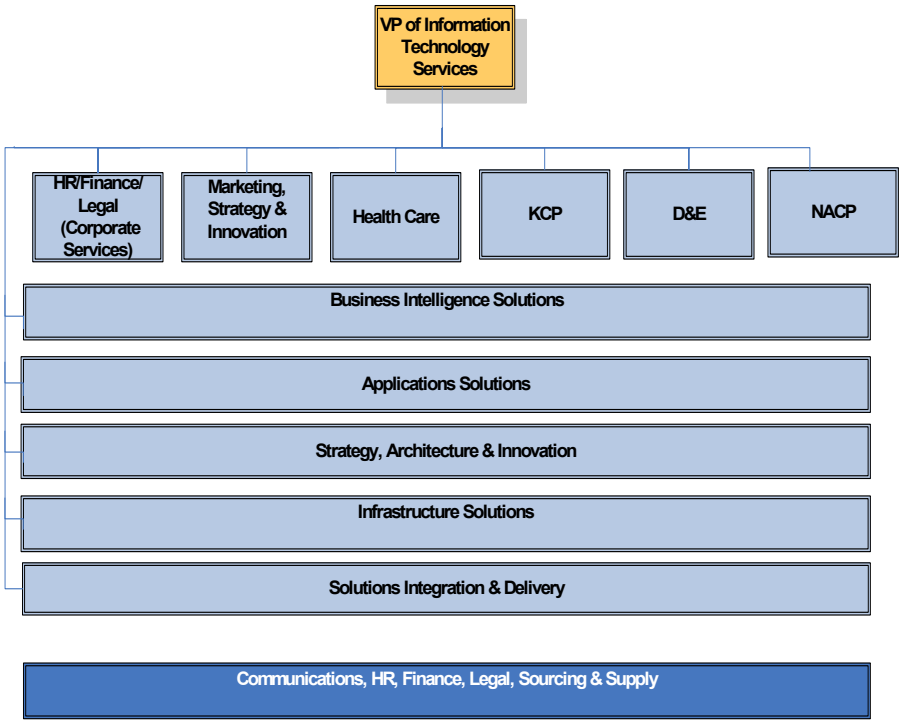
Conocimiento: CCNA Cisco; Plataforma Microsoft Office 2007; Instalación y Recuperación de Hardware y Software; mantenimiento correctivo y preventivo de hardware.

Experiencia: Mínima 2 años en cargos similares.

Habilidades: Trabajo bajo presión, Habilidad numérica, Habilidad analítica, Trabajo en equipo, Trabajo Individual, Responsabilidad, Interacción y Comunicación Social y Orientación a los resultados.

3.2.2. Áreas relacionadas al departamento de IT

Gráfico 3.2: Áreas relacionadas a IT



Fuente: Cía. Clark S.A.

Los principales departamentos relacionados con el departamento de IT son el departamento financiero, marketing, producción y distribución. Están altamente conectados y obtienen los mayores recursos de IT.

3.3. CLASIFICACIÓN Y DETALLE DE LOS PROCESOS DE IT

Los Procesos de IT cumplen con los estándares de la empresa, estos se basan en:

- Adquisición y mantenimiento de software aplicativo
- Instalación y acreditación de los sistemas
- Soporte a los Clientes
- Administración de datos, instalaciones y operaciones
- Administración de problemas e incidentes
- Seguridad de la Información

El Área de IT de se clasifica de la siguiente manera:

HARDWARE:

Instalación, Mantenimiento, reparación y Soporte de los equipos:

- Equipos de networking CISCO (routers y switches)
- Servers (COMPAQ Proliant ML370, Proliant DL380)
- Desktops COMPAQ (Evo D500)
- Laptops (Evo N400c, N600c, N6000c, NC6400)

SOFTWARE:

Actualmente los siguientes módulos de SAP están en uso:

- Requisition to Payment (RTP)
- Forecast To Stock (FTS)
- Accounting To Reporting (ATR)
- Order To Cash (OTC)
- Customer Relationship Management (CRM)

Sistemas desarrollados o administrados localmente:

- Nómina Adams realizado en Visual Basic 6.0 con SQL Server 2000.
- Cubos Locales

TELECOMUNICACIONES:

La tecnología de comunicaciones Frame Relay, ATM, RDSI para conectar Quito y el centro principal de comunicaciones Guayaquil, con un ancho de banda suficiente que proporcione tiempos de respuesta aceptables para la cantidad de información que es transferida.

3.4. PONDERACIÓN DEL ÁREA IT

3.4.1. Análisis de Criticidad

Tabla 3.1: Análisis de Criticidad de IT

Área	Operaciones	Posibles Causas
Hardware	CRÍTICAS	Daño a los equipos por sobrecalentamiento de los procesadores.
	VITALES	Inversión de Hardware no justificable.
	SENSITIVAS	Error en el uso de los equipos por parte de los usuarios.
Software	CRÍTICAS	Error en los procedimientos al momento de generar respaldos o de recuperar información.
		Manipulación de datos por personal no autorizado.
	SENSITIVAS	Ejecutar procesos sin autorización que alteren los registros.
Telecomunicaciones	CRITICAS	Acceso a información por personas no autorizadas.
		Fallas o daños a las redes.
		Falla en la conexión entre localidades.
	VITALES	No disponer del servicio en el tiempo prudente.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

3.4.2. Ponderación de la eficiencia del recurso IT

Tabla 3.2: Ponderación de eficiencia de IT

Áreas	Ponderación		
	Alta	**Media**	**Baja**
Hardware	**x**		
Software	**x**		
Telecomunicaciones	**x**		

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

El área de IT tiene una ponderación alta en cuanto a la eficiencia de los recursos y manejo de la información, así como el debido soporte, mantenimiento, instalación y seguridad de los equipos y programas que cumplen con los estándares de la compañía dando como resultado el óptimo proceso de las operaciones diarias.

CAPÍTULO IV

4. IDENTIFICACIÓN DEL ÁREA DE IT

4.1. ANÁLISIS DE LA INFRAESTRUCTURA

El Área de IT de la Compañía Clark S.A. detalla el inventario que existe en las tres ramas de los Sistemas de Información: Hardware, Software y telecomunicaciones.

- **Hardware**

Servidores:

Tabla 4.1: Modelos de Servidores

Model: COMPAQ Proliant ML370	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	PENTIUM III 1.2 GHZ.
Hard Drives capacity (GB)	12 GB SCSI HARD DISK
Model: COMPAQ Proliant ML370	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 3.1 GHZ INTEL PENTIUM 4 XEON H.T.
Hard Drives capacity (GB)	12 GB SCSI HARD DISK

Tabla 4.1: Modelos de Servidores (Continuación)

Model: HP Proliant DL380	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 3.4 GHZ INTEL PENTIUM 4 XEON H.T.
Hard Drives capacity (GB)	12 - 260 - 140 GB SCSI HARD DISK
Model: HP Proliant DL380	
OPTICAL DRIVE	CD-ROM
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 3.4 GHZ INTEL PENTIUM 4 XEON H.T.
Hard Drives capacity (GB)	12 GB SCSI HARD DISK
Model: HP Proliant DL380	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 3.4 GHZ INTEL PENTIUM 4 XEON H.T.
Hard Drives capacity (GB)	12 - 260 - 140 GB SCSI HARD DISK
Model: HP Proliant DL380	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 3.4 GHZ INTEL PENTIUM 4 XEON H.T.
Hard Drives capacity (GB)	12 - 260 - 140 GB SCSI HARD DISK

Tabla 4.1: Modelos de Servidores (Continuación)

Model: COMPAQ Proliant ML370	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	2 GB
CPU model/speed	DUAL 1.3 INTEL PENTIUM 3
Hard Drives capacity (GB)	15 - 12 - 125 GB SCSI HARD DISK
Model: COMPAQ Proliant ML370	
OPTICAL DRIVE	CD-ROM
FLOPPY	FLOPPY DISK
Operating System	WINDOWS SERVER 2003 SP1
RAM	1 GB
CPU model/speed	PENTIUM III 1.2 GHZ.
Hard Drives capacity (GB)	18 GB SCSI HARD DISK

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Información de Respaldo por Servidor:

Tabla 4.2: Respaldo por Servidor

#	Host Name	Location	Use	Team Responsible	Offsite Media Location	Media Type	LAN Backup Time	Instance Backing Up	Restore Type/ Ave. GB/Hr	Backup Frequency	Used Space GB	Average Restore Time Hr
1	**ECGUFN01**	Guayaquil	File & Print		Caja de Seguridad/Bco. Bolivariano	SDGLT 200/400	3 Hrs	VERITAS	30 GB	Diarios, Semanales y Mensuales.	70 GB	2 Hrs.
2	**ECGUAX02**	Guayaquil	Mail		Caja de Seguridad/Bco. Bolivariano	SDGLT 200/400	2 Hrs	VERITAS	20 GB	Diarios, Semanales y Mensuales	180 GB	1 Hrs.
3	**ECGUFN02**	Guayaquil	Backup									
4	**ECGUNDC0**	Guayaquil	Domain Controller									
5	**ECGUASM1**	Guayaquil	Sms/Software Package									
6	**ECGUAS02**	Guayaquil	Central Telefónica									
7	**ECGUAF01**	Guayaquil	Fax Server									
8	**ECGUAS01**	Guayaquil	Application Server		Caja de Seguridad/Bco. Bolivariano	SDGLT 200/400	2 Hrs	VERITAS	20 GB	Diarios, Semanales y Mensuales	180 GB	1 Hrs.
9	**ECGUAS01-N**	Guayaquil										
10	**ECQTNDC0**	Quito	Domain Controller									
11	**ECQTFN01**	Quito	File & Print		Caja de Seguridad/Bco. Bolivariano	180/360	1 Hr	VERITAS	20 GB	Diarios, Semanales y Mensuales.		3 Hrs.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Printers:

Tabla 4.3: Inventario de Impresoras

NOMBRE	IP	COMENTARIO	UBICACION	MODELO	DRIVERS
ECGUP001	172.25.84.201	CAJA - (SAP)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON FX-1180
ECGUP002	172.25.84.202	MATRICIAL (ventas notas de debito)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON FX-1180
ECGUP006	172.25.85.203	LOGISTICA (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345
ECGUP012	172.25.85.200	FINANZAS (CONTABILIDAD, COSTOS, COBRANZAS, TESORERIA)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345
ECGUP015	172.25.84.215	VENTAS CONSUMO - (SAP)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON DFX-8500
ECGUP016	172.25.84.235	LOGISTICA, GUIAS KCP- (SAP)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON DFX-8500
ECGUP020	172.25.84.205	CREDITO - (SAP)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON DFX-8500
ECGUP023	172.25.84.243	IMPORTACIONES - (SAP)	GUAYAQUIL, ECUADOR	MATRICIALES	ESERIES PCLON FX-1180
ECGUP033	172.25.85.200	FINANZAS - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345 SERIES PCL
ECGUP034	172.25.85.201	VENTAS - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345 SERIES PCL
ECGUP035	172.25.85.202	NOMINA	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP036	172.25.85.203	LOGISTICA - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345
ECGUP037	172,25,85,204	SUPERVISORES DE PLANTA - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP038	172.25.85.205	PRODUCCION C. CALIDAD - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP039	172.25.85.206	GERENCIAS - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345 SERIES PCL

Tabla 4.3: Inventario de Impresoras (Continuación)

NOMBRE	IP	COMENTARIO	UBICACION	MODELO	DRIVERS
ECGUP040	172.25.85.207	COMPRAS - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345 SERIES PCL
ECGUP041	172.25.85.208	BODEGA M. PRIMA - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP042	172.25.84.251	GERENCIA FINANCIERA - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP043	172.25.84.253	GERENCIA VENTAS - (SAP)	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP044	172.25.85.209	VENTAS KCP	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASERJET 4000 SERIES PCL
ECGUP045	172.25.84.211	LOGISTICA	GUAYAQUIL, ECUADOR	HP LASER MF345	HP LASER MF345 SERIES PCL

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Servidores de Repuesto:

Tabla 4.4: Servidores de Repuesto

Server Name	**ECGUFN02**
Server Model	Compaq Proliant ML370
Server Description	DC & SMS Secondary or Contingecy Server
Server Role	BDC
Operating System	Windows Server 2003
Workgroup/Domain	KCUS
Server Stage	OFF
Building	M.I.S. Office (Computer Center)
Site server will be built	M.I.S. Office (Computer Center)
IP to build with	Must supply a temp ID if the request is for a BDC
Supported By	INTERNATIONAL MIS
System Owner	Clark S.A.
RAM	768 MB
CPU model/speed	1.3 GHz Pentium III
NIC	HP NC3163 Fast Ethernet NIC
IP for NIC	
SN# (Required)	D150FRV1K063
Hard Drives Qty.	5
Hard Drives capacity (GB)	36.4
Remote Management (iLO)	Yes
Generation	G3
KCC S/Number	53500316
Owner	Carlos Pelaez

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- **Software:**

Aplicativo de Nómina ADAMS, realizado en Visual Basic 6.0 con SQL Server 2000.

Proceso SAP (Planificación de Recursos Empresariales)

Microsoft SQL Server 2000

Microsoft Office 2007

Todos los paquetes adquiridos y utilizados en la compañía Clark S.A. se registran con licencia corporativa que es adquirida por la misma para poder utilizarla en todas sus filiales a nivel mundial.

De acuerdo a estándares corporativos no se debe utilizar ningún software Open Source por seguridad de la empresa.

- **Telecomunicaciones:**

Switch y Routers:

Tabla 4.5: Inventario de Switch y Routers

Location	Name	Category	Serial Number	O/S Information	Model	IP Address	Subnet Mask
	CI-NAME	**CI-CATGRY**	**CI-SN**	**CI-OS-INFO**	**CI-MODEL**	**CI-IP**	**CI-SUB-MSK**
	SMARTS	SMARTS	Manual entry	SMARTS	SMARTS	Manual entry	Manual entry
	Required? – Yes	Required? - Yes	Required? - Yes	Required? - Yes	Required? - Yes	Required? - Yes	Required? - Yes
SISTEMAS	ECGUCR1	Router	JHY0834K01A	Version 12.3(5c)	C3725-IPVOICE-M	172.25.84.254	255.255.254.0
SISTEMAS	ECGUNS1	Switch	FOC0843W12F	Version 12.1(22)EA1	WS-C2950G	172.25.84.221	255.255.254.0
SISTEMAS	ECGUNS2	Switch	FAB0546P06Z	Version 12.0(5.3)WC(1)	WS-C3548	172.25.84.222	255.255.240.0
SISTEMAS	ECGUNS3	Switch	FAB0546Q08Y	Version 12.0(5.3)WC(1)	WS-C3548	172.25.84.223	255.255.240.0
KCP	ECGUNS4	Switch	FAB0545Q22T	Version 12.0(5.3)WC(1)	WS-C3548	172.25.84.224	255.255.240.0
KCP	ECGUNS5	Switch	FAB0546P06T	Version 12.0(5.3)WC(1)	WS-C3548	172.25.84.225	255.255.240.0
CONTROL DE CALIDAD	ECGUNS6	Switch				172.25.84.226	255.255.240.0
LOGISTICA	ECGUNS7	Switch	FOC0833X1WT	Version 12.1(22)EA6	WS-C2950G	172.25.84.217	255.255.240.0
SALA CAP. 2	ECGUNS8	Switch	FOC0833X1XH	Version 12.1(11r) EA1	WS-C2950G	172.25.84.240	255.255.240.0
LIBRE	ECGUNS9	Switch	FOC0833X1XJ	Version 12.1(11)EA1	WS-C2950G-48	172.25.84.241	255.255.240.0
LIBRE	ECGUNS11	Switch	FAA040F1EQ	Version 12.0(5) WC3b	WS-C3524-XL-EN		
KCP	ECGUNS10	Switch	FOC0646S05N		WS-C2950G-24	172.25.84.244	
BABAHOYO	ECBACR1	Router	26759573	Version 12.2(12a)	C3640-IS-M	172.25.87.254	255.255.255.0
BABAHOYO	ECBANS1	Switch	FAB0546P071	Version 12.0(5.3)WC(1)	WS-C3548-XL-EN	172.25.87.254	255.255.255.0
QUITO	ECQTCR1	Router	JHY0726K039	Version 12.2(12a)	C2600-IS-M	172.25.86.254	255.255.240.0
QUITO	ECQTNS1	Switch	FAB0546P06Q	Version 12.0(5.3)WC(1)	WS-C3548-XL-EN	172.25.86.253	255.255.255.0

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Tarjetas RAS:

Tabla 4.6: Inventario de Tarjetas RAS

No	Localidad	Usuario	Area	Proceso	ID	PIN	ID Ras	Status
48	Guayaquil	Gonzalez, Danny	Finanzas	Finanzas	C11401		**30718999**	Operativa
58	Guayaquil	Isidro Reyes	Ventas	Ventas	C12134		**39059363**	Operativo
16	Guayaquil	Jaime Ferrer	Produccion	Produccion	L40017			Operativa
59	Guayaquil	Isasi, Rodrigo	Ventas	Ventas	L60160		**39059367**	Operativo
8	Guayaquil	Diego Alvarez Del Villar	Mercadeo	Mercadeo	L60193		**30735408**	Operativa
61	Guayaquil	Gonzalez, Alejandro	Ventas	Ventas	L71391		**21022485**	Operativo
11	Guayaquil	Geovanni Tapia	LAO	LAO	L80029			Operativa
29	Guayaquil	Maria Sol Solines	Mercadeo	Mercadeo	L80047		**30718998**	Operativa
38	Guayaquil	Rafael Hincapie	KCP	KCP	L80096		**30735399**	Operativa
23	Quito	Ketty Mariano	Ventas	Ventas	L80152	8015	**30735398**	Operativa
28	Quito	Maria Sol Cepeda	Mercadeo	Mercadeo	L80322	8032	**30735405**	Operativa
43	Guayaquil	Sergio Cruz	Presidencia	Presidencia	L80329			Operativa
32	Guayaquil	Monica Costa	Mercadeo		L80330			Operativa
19	Guayaquil	Jorge Bustamante	Mercadeo	Mercadeo	L80334		**30719003**	Operativa
14	Guayaquil	Homero Lucio	Sistemas	Sistemas	L80335	1263	**27647511**	Operativa
1	Guayaquil	Adrian Arroba	Mercadeo	Mercadeo	L80343		**30719005**	Operativa
56	Guayaquil	José Santos	Ventas	Ventas	L80409		**39059368**	Operativo
34	Guayaquil	Oscar Gamarra	LAO	LAO	L83002			Operativa

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

4.2. DESCRIPCIÓN DE PROVEEDORES DE SERVICIOS EXTERNOS

La compañía Clark S.A. requiere los servicios personalizados de proveedores externos que contribuyan a la calidad de sus funciones y orientados a alcanzar los objetivos corporativos.

La función al contratar un proveedor externo para el área de IT es brindar apoyo intelectual a la compañía. La empresa cuenta con sistemas y equipos suficientes para las operaciones diarias, esta provee las herramientas necesarias a los operadores de empresas Outsourcing.

A continuación se detalla la tabla 4.7. que muestra la lista de empresas proveedoras externas con su respectivo líder.

Tabla 4.7: Proveedores de Servicios Externos

Título	Nombre
IMSERIES PCLAT Proveedor de Enlace Nacional	Enrique Erazo
PACIFICTEL Proveedor de Enlaces Internacionales	Marcia Moreno
TRANSFERDATOS Proveedor de Ultima Milla	Eladio Vera
INFONET Proveedor de Enlaces Internacional-Quito	Ramiro Rodas

Tabla 4.7: Proveedores de Servicios Externos (Continuación)

Título	Nombre
SONDA del Ecuador Proveedor de Equipos, Partes HP	Xavier Robles
SYSTELECOM Proveedor Soporte en Telefonía	Luis Caiza
TELEFONICA Proveedor Soporte Equipos Comunicación	Darío Ojeda

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Repuestos de Equipos:

Antecedentes.-

Según contrato de servicios firmado el 2 de junio del año 2005 entre CLARK S.A., en calidad de Cliente y la Compañía TELEFONICA S.A., ECUAPHONE, en calidad de Proveedor, Clark S.A. obtendrá los servicios de Soporte técnico, mantenimiento y backup de equipos de comunicación durante la vigencia del mencionado contrato.

Descripción de Servicios:

Telecomunicaciones

- **Equipos de Backup**

Tabla 4.8: Equipos Backup

Cantidad	Equipo	Marca	Modelo
1	Routers	Cisco	1700
1	Routers	Cisco	3640
1	Switch	Cisco	Catalyst WS-C3524

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- **Equipos cubiertos con Soporte y Mantenimiento (On Site)**

Tabla 4.9: Equipos On Site

Cantidad	Equipo	Marca	Modelo
1	Routers	Cisco	2650MX
1	Routers	Cisco	3640
1	Routers	Cisco	3725
1	Switch	Cisco	Catalyst 3524
4	Switch	cisco	Catalyst 3548
4	Switch	cisco	Catalyst 2950G-48
1	Switch	cisco	Catalyst 2950G-24
1	Access Point	cisco	1231

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

4.3. Análisis del Costo de la Infraestructura

En está sección analizamos el costo de operación que resulta invertir en un plan de continuidad de negocio (BCP) para la Cía. Clark S.A., para el cuál evaluamos si conviene o no invertir en un BCP. Para esto resolvemos la siguiente fórmula donde nos indica el costo de invertir en un BCP sobre el stock del producto final que es el core business de la compañía.

Tabla 4.10: Detalle de Cuentas

Detalle Cuentas	Saldos
Ingresos	27,830,320.31
Family Care 40%	11,132,128.12
Papel Higiénico 87%	9,684,951.47
Costo de BCP	139,824.60

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

$$Costo\ de\ Operación = \frac{Costo\ de\ BCP}{Stock\ del\ \text{Pr}oducto\ Final}$$

$$Costo\ de\ Operación = \frac{139{,}824.60}{9{,}684{,}951{,}46788}\ X\ 100 = 1.44\% \Rightarrow \%\ Costo\ Beneficio.$$

El presupuesto del proyecto es bajo 1.44% con respecto a lo que voy a proteger, es decir invierto $139,824.60 en implementar un BCP para la compañía que prevenga cualquier contingencia que provoque la interrupción de las actividades diarias del negocio para proteger $9,684,951.47 que es el core business del negocio.

Además analizamos el % de rentabilidad que nos permite estar asegurar si conviene o no invertir en un BCP.

$$\%\, Utilización\ de\ \mathrm{Re}\, ntabilidad = \frac{Costo\ de\ BCP}{Utilidad}$$

$$Costo\ de\ Operación = \frac{139{,}824.60}{27{,}830{,}320.31}\ X\ 100 = 0.50\%$$

Como se observa al resolver la fórmula vemos que el valor no es tan representativo con respecto a la rentabilidad o beneficio neto que me queda. El 0.50% es porción que tomo de los beneficios netos para proteger mi negocio. Lo cuál resulta conveniente invertir en un BCP para la compañía como se ha mostrado, ya que el beneficio es mayor al costo que genera la inversión. Aunque está decisión la puede tomar el ejecutivo de la compañía ya que el valor no es representativo, en caso de que fuera representativo lo evalúan los accionistas de la compañía.

CAPÍTULO V

5. FABRICACIÓN Y PRODUCCIÓN

5.1. PORTAFOLIO DE PRODUCTOS

La Compañía Clark S.A. ofrece lo último en innovación, tecnología y la más alta calidad mediante la comercialización de todos los productos. Diariamente contribuye a la satisfacción y al bienestar de los consumidores ecuatorianos a través de la difusión de la higiene y la limpieza para bienestar de los clientes.

Existen dos divisiones comerciales: De consumo con las Categorías de Cuidado Familiar y la otra división comercial es la de productos institucionales Clark Profesional.

A continuación clasificamos los productos en las siguientes categorías como muestra la tabla:

Tabla 5.1: Portafolio de Productos

PRODUCTOS	CATEGORIAS
Papel Higiénico	Papel Higiénico Jumbo. Papel Higiénico Bulk pack. Papel Higiénico Convencional.
Servilletas	Servilletas dispensadas. Servilletas convencionales. Servilletas de lujo.
Toallas de Mano	Toallas de Mano dobladas. Toallas de Mano en rollo vertical. Toallas de Mano en rollo horizontal.
Pañuelos Faciales	Pañuelos Faciales 100 hojas – caja grande. Pañuelos Faciales 65 hojas – caja pequeña.
Pañuelos Faciales	Pañuelos Faciales 100 hojas – caja grande. Pañuelos Faciales 65 hojas – caja pequeña.
Jabones	Jabones uso personal. Jabones antibacterial. Jabones uso industrial.
Toallas desechables	Toallas desechables para el cuerpo Toallas desechables funda

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

5.2. PROCESO DEL PRODUCTO ESTRELLA

La empresa elabora su producto principal que se convierte en sinónimo de suavidad, calidad, limpieza, cuidado y confort. El objetivo de la compañía es el de fabricar un papel de superior calidad, confeccionado enteramente con hebras de lino y algodón.

El proceso de confección del papel sanitario se realiza continuamente, a través de una máquina que se alimenta de pulpa y de los aditivos correspondientes, y produce rollos de papel de las características deseadas.

Primero se bombean las materias primas que son las fibras y los aditivos químicos con agua a la cabeza de máquina, la cual alimenta continuamente la sección de mallas, que es una cinta larga y elástica (de hasta 35 m de longitud) y cuyo ancho es el de la máquina. El agua que acompaña a la pulpa comienza a escurrirse por los huecos de la maya, arrastrando consigo las fibras más finas las cuál son reaprovechadas más tarde. Se pierde un alto porcentaje del agua que contiene la pulpa, cuando la pulpa llega al final de la cinta de mallas, se ha convertido en una hoja de papel, pero aún muy húmeda y de muy baja resistencia.

Luego se pasa al área de prensado, que está formada por una serie de cilindros pesados a través de los cuales pasa el papel húmedo. En ellos, la humedad es escurrida y retirada por succión. Después el papel pasa al área de secado. En está área existen un gran número de cilindros desecadores, calentados por vapor a una temperatura ligeramente superior a los 100ºC. La hoja de papel pasa a través de estos cilindros hasta que el papel se seque completamente. En la parte final del banco de cilindros se encuentra el área de calandrado, que consiste mejorar el acabado del papel mejorando la lisura de la superficie y haciendo el papel más brillante. El tratamiento se efectúa en la satinadora, máquina compuesta por cilindros de hierro colado con la superficie dura y brillante y cilindros con fibra con la superficie elástica y compresible.

La siguiente área es el estucado, que es una operación donde se modifican las características del papel permitiendo mejorar los resultados de la impresión y alcanzando un mayor grado de blancura. El proceso consiste en aplicar sobre una de las caras del papel una capa de adhesivos y pigmentos que forman una película de barniz (el estuco) que da al papel gran finura y uniformidad.

Una vez obtenida la pulpa de papel en condiciones adecuadas para la confección del tipo de papel deseado se realiza la conversión a papel sanitario.

5.3. SECTORES Y PROMESA DE VENTA

- ✓ **Sector Oficinas**

  Brindamos soluciones innovadoras para mejorar el ambiente de trabajo haciendo que sus empleados se sientan a gusto y que sus clientes se lleven la mejor impresión.

  - Satisfacción para su gente
  - Imagen en su empresa
  - Calidad y rendimiento

- ✓ **Sector Industrial**

  Le damos soluciones versátiles para mejorar la productividad y eficiencia de su negocio.

  - Hacemos “más con menos”
  - Eficiencia para maquinarias
  - Seguridad a sus empleados

- ✓ **Sector Salud**

  • Proporcionamos un ambiente altamente higiénico para evitar que las áreas de atención a sus pacientes no tengan riesgo de contagio.

  • Seguridad a pacientes y visitantes.

  • Seguridad en su lugar de trabajo.

- ✓ **Sector Hotelería y Turismo**

  Ponemos los detalles que hacen que sus huéspedes se sientan como en casa.

  • Satisfacción para sus huéspedes, clientes e invitados.

  • Imagen

- ✓ **Sector Procesadora de Alimentos y Restaurantes**

  • Los alimentos que ingerimos deben estar procesados con calidad, ayudamos para que el proceso tenga la garantía de higiene que su negocio necesita y sus clientes buscan.

  • Seguridad, Imagen, Calidad y Servicio.

- ✓ **Sector Alto Tráfico**

  Somos capaces de atender de manera higiénica y segura a un gran número de personas con sistemas que resisten el uso y el abuso.

  • Confianza y seguridad

  • Alto rendimiento

5.4. ANÁLISIS DE PRODUCTIVIDAD

El análisis del índice de productividad nos muestra la eficiencia operativa de la misma. Detallamos y calculamos los siguientes parámetros de rentabilidad, tomamos los valores de los Estados Financieros, tanto el Balance General y el Estado de Pérdidas y Ganancias al 31 de Diciembre de 2008 para el cálculo, los cuáles se muestran en la siguiente tabla:

Tabla 5.2: Saldos de los Ef´s

CUENTAS EF´S	SALDOS
Ventas	104,398,975.48
Costo de Ventas	76,568,655.17
Utilidad Neta	27,830,320.31
Activos Fijos Netos	10,306,300.26
Total Activos	65,817,136.20

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Margen de Utilidad:

$$ROS = \frac{Ventas - Costo\,de\,Ventas}{Ventas} = \frac{104{,}398{,}975.48 - 76{,}568{,}655.17}{104{,}398{,}975.48} = 0.26 = 26\%$$

Este valor indica que la empresa ganó 42 centavos por cada venta que realiza pagado todos sus productos.

Rotación de Activos Fijos:

$$ROE = \frac{Ventas}{Activos\ \ Fijos\ \ Netos} = \frac{104{,}398{,}975.48}{10{,}306{,}300.26} = 10.13\ veces$$

Este valor indica que la empresa rota sus activos 10.13 veces al año.

Retorno sobre Activos (Inversión):

$$ROI = \frac{Utilidad\ \ \ Neta}{Total\ \ \ Activos} = \frac{27{,}830{,}320.31}{65{,}817{,}136.20} = 0.42 = 42\%$$

Este valor indica que la empresa ganó 42 centavos por cada dólar de inversión en activos.

Leyenda:

ROS: Parámetro que mide la rentabilidad sobre las ventas que realiza.

ROE: Parámetro que mide el rendimiento sobre sus activos fijos.

ROI: Parámetro que mide el rendimiento de la inversión sobre el activo total.

Análisis:

La compañía Clark S.A. muestra un retorno de rentabilidad alto sobre las ventas (26%), esto indica un buen control sobre sus costos. Su retorno sobre activos es del (42%), lo cuál significa que la compañía, rota más rápido sus activos, es decir mantiene el uso eficiente de los activos en el balance general.

La empresa mantiene un índice de ventas muy elevado (10.13 veces) sobre sus activos fijos (planta y equipo), lo cuál indica de nuevo que rota rápidamente los activos. La utilidad de la compañía es alta, muestra liquidez y rentabilidad. Su nivel de productividad es alto, lo cuál emplea la mano de obra y el equipo en la forma más eficiente y al costo más bajo.

CAPÍTULO VI

6. FASE DE RECUPERACIÓN

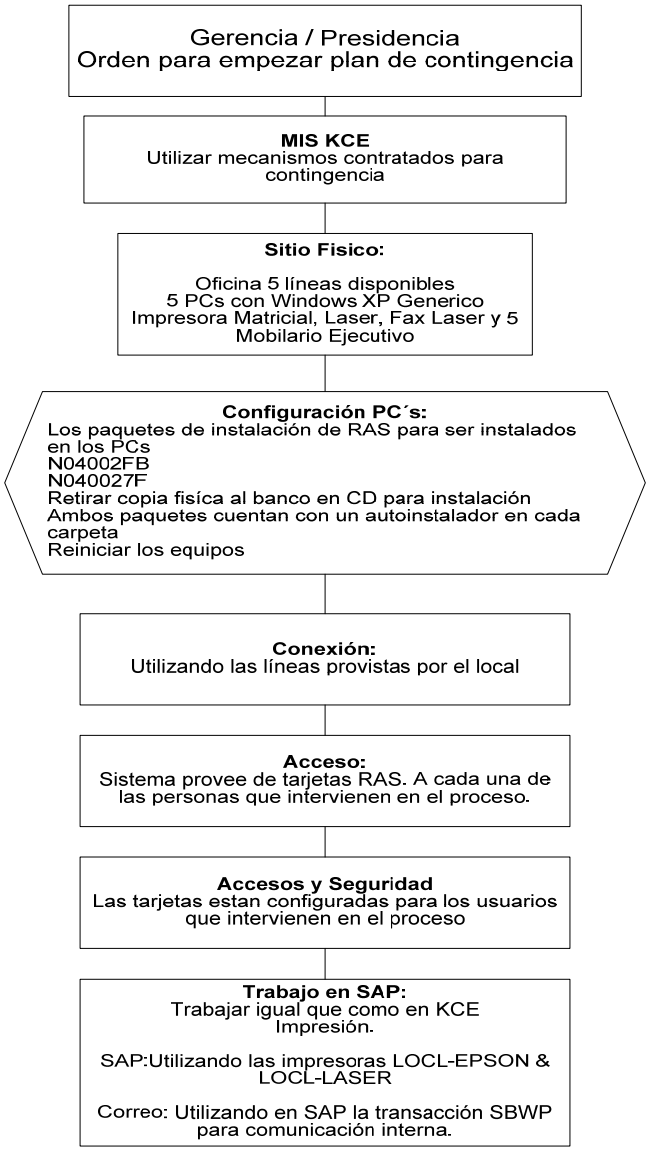
6.1. ESTRATEGIA DE RECUPERACIÓN

La Administración ha reconocido las pérdidas potenciales asociadas con una interrupción de las operaciones de ITS, así como la importancia de mantener estrategias de continuidad viables para mantener el servicio de MIS disponible para nuestros clientes. Para que un Plan de Continuidad sea útil, debe tener estrategias desarrolladas para 1) comunicar, controlar el proceso de reanudación, asegurar que el personal sea capaz de ejecutar sus responsabilidades, y 2) obtener el hardware para el procesamiento en un tiempo oportuno, así como de definir localidades alternas para el procesamiento y asegurar que la información respaldada pueda ser obtenida y procesada efectivamente.

Estas oficinas han implementado ó están en el proceso de revisión de las estrategias para la reanudación de sus operaciones críticas, funciones de procesamiento computarizado así como de su infraestructura de hardware.

Una vez de que la gerencia indique a ITS la decisión de proceder con los trabajos de recuperación se mantendrá el siguiente esquema de comunicación.

Gráfico 6.1: Diagrama Paso a Paso de Recuperación



Fuente: Clark S.A. Ver Anexo 3: Simbología

Tabla 6.1: Estrategia de Recuperación

Categoría	Estrategia de Recuperación
Notificación del Incidente	El Gerente encargado del Sitio (Oficina Central o Planta de producción) o el Administrador de LAN notificarán al personal si una situación de desastre ocurre en la Planta. El Plan de Continuidad de Negocios contiene una "Lista de control para Potenciales Desastres de MIS" para determinar si hay una situación de desastre de MIS. En la notificación del incidente, el Administrador de LAN se encontrará en la Planta con el propósito de realizar una valoración preliminar para comunicar a la gerencia de planta del estado de la emergencia. El Administrador de LAN comenzará las actividades contenidas en el Plan de Continuidad de Negocios, para determinar si un desastre necesita ser declarado y las actividades de reanudación necesitan ser activadas.
Notificación al Personal Interno	El Plan de Continuidad de Negocios se usará para la notificación del personal de MIS y Administrativo, en relación a las acciones específicas a ser tomadas. El Gerente de planta notificará al Gerente General si el evento constituye una crisis o una potencial crisis, el Gerente de planta tomara acciones apropiadas definidas en el Procedimiento de Respuesta para Averías Específicas de MIS o la sección de Sabotaje u otras secciones incluidos en los Procedimientos corporativos sobre administración de crisis.
Notificación Externa	Existen clientes externos que requieren ser notificados. Los números de contactos estarán contenidos en el plan de Continuidad de Negocio.
Localización del Control de la Emergencia	Existen en Ecuador dos sitios (Oficina Quito y Oficina de Fibra Secundaria) que pueden ser usados como un centro de control para administrar los incidentes de desastre.
Ejercicios de prueba	Las aplicaciones críticas serán probadas en servidores alternos anualmente. MIS realizará una revisión anual con el personal apropiado.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Tabla 6.2: Estrategia de Recuperación de Hardware

Categoría	Categoría detallada	Estrategia de Recuperación de Hardware	Localidad de Reanudación	Método de Backup Archivos	Localidad de Almacenamiento de Backup
Mainframe		N/A			
AS/400		N/A			
Windows 2003	ECGUFN01 ECGUAX02 ECGUFN02 ECGUNDC0 ECGUASM1 ECGUAS02 ECGUAF01 ECGUAS01 ECGUAS01-N ECQTNDC0 ECQTFN01	El proveedor Leasing de SONDA/HP, enviara el servidor o las partes que se requieran para tener el servidor en óptimas condiciones. El administrador de la red en conjunto con el “Enterprise Server Team” de Clark S.A. se encargara de reinstalar el sistema operativo.	Todos los archivos de datos serán restaurados en el servidor de reemplazo por el administrador local; las cintas de respaldo se encuentran en un sitio fuera de la compañía en el casillero del Banco Bolivariano.	VERITAS	Banco Bolivariano, casillero 44B

Tabla 6.2: Estrategia de Recuperación de Hardware (Continuación)

Categoría	Categoría detallada	Estrategia de Recuperación de Hardware	Localidad de Reanudación	Método de Backup Archivos	Localidad de Almacenamiento de Backup
Comunicaciones de Datos	Routers ECGUFNR1 ECGUFNR2	Los Routers están incluidos en un contrato SMART NET, el proveedor SONDA, enviara el router en un plazo máximo de 1 dias; El coordinador de infraestructura en conjunto con el Network Management team se encargara de reinstalar el equipo.	El coordinador de infraestructura realizara el procedimiento necesario para que el Network Management team instale la configuración del Router.		Clark-UIO
	CSU/DSU	El proveedor SONDA reemplazara el CSU/DSU en un plazo máximo de 24 horas, con el fin de garantizar que el circuito Frame Relay este operativo.	El proveedor SONDA instalara el nuevo CSU/DSU en el sitio específico.		SONDA ver lista de contactos, Sect App K.
	Console Modems	El coordinador de infraestructura suministrara el MODEM de consola, en un plazo máximo de 48 horas después de estar declarada la situación de desastre; este equipo es requerido para acceder el Router.	El coordinador de infraestructura instalara el nuevo MODEM de consola en el sitio específico.		Departamento de Sistemas.

Tabla 6.2: Estrategia de Recuperación de Hardware (Continuación)

Categoría	Categoría detallada	Estrategia de Recuperación de Hardware	Localidad de Reanudación	Método de Backup Archivos	Localidad de Almacenamiento de Backup
	Facility Modems	El departamento de sistemas tendrá en inventario módems que serán utilizados para reemplazar los equipos que se destruyan en el desastre.	El coordinador de infraestructura instalara el nuevo MODEM de consola en el sitio específico.		Departamento de Sistemas.
	Switches	Los Switches están incluidos en un contrato SMART NET (ver Sect App T), el proveedor SONDA, enviara el Switche en un plazo máximo de 1 dia; el coordinador de infraestructura se encargara de reinstalar el equipo.	El coordinador de infraestructura instalara el nuevo Switche en el sitio específico.		SONDA
	Cable Infrastructure	El proveedor SONDA reemplazara los cables de Fibra Optica, controllers, router y cable para CSU/DSU en un plazo máximo de 24 horas después de estar declarada la situación de desastre.	El proveedor SONDA instalara el nuevo cable para CSU/DSU, controllers o routers, en el sitio especifico.		SONDA

Tabla 6.2: Estrategia de Recuperación de Hardware (Continuación)

Categoría	Categoría detallada	Estrategia de Recuperación de Hardware	Localidad de Reanudación	Método de Backup Archivos	Localidad de Almacenamiento de Backup
Impresoras	ECGUP011 ECGUP012 ECGUP013 ECGUP014 ECGUP015 ECGUP016 ECGUP017 ECGUP018 ECGUP019 ECGUP003	El proveedor HP reemplazara las partes o las impresoras en el momento que se requiera en un plazo máximo de 24 horas después de estar declarada la situación de desastre.	Hasta que la impresora sea reemplazada, todos los archivos que el usuario requiere imprimir deben ser enviados a otra impresora del sitio específico o a otra impresora en otra ubicación.		Departamento de compras.
PCs		El proveedor Leasing SONDA, enviara los PC'S o las partes que se requieran para tener el PC en óptimas condiciones. El administrador de la red se encargara de reinstalar el sistema operativo.	Todos los archivos de datos serán restaurados en el PC de reemplazo por el administrador local; las cintas de respaldo se encuentran en un sitio fuera de la compañía en el Banco B.		Banco Bolivariano.

Tabla 6.2: Estrategia de Recuperación de Hardware (Continuación)

Categoría	Categoría detallada	Estrategia de Recuperación de Hardware	Localidad de Reanudación	Método de Backup Archivos	Localidad de Almacenamiento de Backup
UPS	FV Best 35 kva Centro de Computo servidores	El proveedor Cotel suministrara el servicio y soporte para reparación o el cambio de las partes que se requieran para el optimo funcionamiento del equipo.	La alimentación del sistema regulada el centro de computo principal esta conectado al generador principal de emergencia como contingencia para la UPS de 35Kva.		Proveedor Cotel ver lista de contactos, Sect App K.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

6.1.1. Procedimiento de Contingencia para transporte de Equipos

Procedimientos de embarque de equipos (Router, switches, cintas, provisiones, etc.) para una instalación en la cual se pueda activar la contingencia.

En la oficina de Quito se cuenta con la infraestructura necesaria para conectar el router con el fin de tener activos todos los enlaces nacionales; para llevar a cabo con éxito esta contingencia se deben seguir los siguientes pasos:

1. Contactar proveedor de equipos y telecomunicaciones (SONDA)
2. Contactar personal de Network Team en Clark S.A.
3. Contactar empresa para transportar y empacar los equipos (Servientrega)
4. Contactar coordinador administrativo oficina Quito
5. Contactar agencia de Viajes (TAME)
6. Enviar equipos
7. Trasladar personal de MIS

6.1.1.1. Procedimiento de Notificación

Contactar el Gerente General y notificarle que la oficina se encuentra en una situación de emergencia y que se esta activando el plan de contingencia. Se debe mirar la lista de información de contactos.

6.2. MANUAL DE ADMINISTRACIÓN DE CRISIS

6.2.1. Plan de Unidad

Una crisis se define como algún evento el cual:

- Envuelve pérdidas de vida reales o potenciales o heridas serias a clientes, empleados u otros afectados por las operaciones de la compañía; o

- Causa daños importantes a los activos de la compañía y necesariamente causa al menos una interrupción temporal de la producción normal de la unidad afectada; o

- Presenta un posible efecto adverso significante a las operaciones continuas de la compañía, reputación de los negocios o resultados financieros.

El equipo central decidirá si un evento particular es una crisis, si es así, debería ser manejado bajo este procedimiento o un procedimiento de la Unidad.

Los siguientes son ejemplos de eventos que pueden ser considerados como crisis corporativa. Esta lista no comprende todo y se incluye únicamente cómo una guía:

- Fuego o explosión mayor en las instalaciones manufactureras, envolviendo muertos o heridos graves y la necesaria cesación de operaciones en esa instalación.

- Recepción de informes indicando que los clientes de CLARK S.A. pueden estar en peligro por el uso de uno de los productos de la Corporación, como resultado de un defecto de manufactura o como resultado de falsificación de los productos.

- Un escape de gas tóxico, derrame de químico, u otro evento similar afectando una comunidad localizada donde hay instalaciones de CLARK S.A.

- Violencia Civil, Desastres Naturales.

6.2.2. Principios de Administración de Crisis

Es la intención de la Corporación planear anticipadamente y estar preparado a intervenir rápida y positivamente con crisis que afectan a CLARK S.A. o sus operaciones en cualquier lugar del mundo

La Planeación de Administración de crisis dentro de CLARK S.A. es importante para hacer énfasis de:

- Prevenir la ocurrencia de un evento de crisis;
- Asuntos prominentes con respecto a consumidores, clientes, empleados y seguridad de la comunidad;
- Mantener la alerta y responder oportunamente a signos de alarmas de posibles eventos de crisis;
- Reportes internos rápidos y exactos de la ocurrencia de eventos de crisis y comunicación completa, exacta y oportuna de la información relacionada con tales eventos dentro la corporación y para el público en general;
- Protección de la reputación de los negocios y activos de la corporación;
- Continuidad de las operaciones de la corporación las cuales no son afectadas por un evento de crisis y

- Buena voluntad para aprender de eventos de crisis pasados y un compromiso para continuar mejorando en la futura planeación de administración de crisis.

6.2.3. Preparación Anticipada

Han sido desarrollado procedimientos de respuesta para categorías específicas de crisis potenciales (“Procedimientos de Respuesta”). Estos procedimientos de respuesta incluyen los pasos iniciales de respuesta a la crisis, una lista de contactos claves internos y externos y sus responsabilidades y una lista de chequeo de asuntos específicos a ser dirigidos. Procedimientos de respuesta para otras categorías de crisis serán desarrolladas cuando el Equipo Central lo considere necesario.

Cada unidad debe desarrollar un plan de respuesta a la crisis el cuál tiene como propósito:

1. La prevención de eventos de crisis en primera instancia,
2. Una respuesta a un evento de crisis si ocurriera.

6.2.4. Procedimiento de respuesta a crisis corporativa

Los pasos para reportar y administrar una crisis son los siguientes:

6.2.4.1. Informe al equipo central de la crisis

- Cualquier persona que identifique una crisis (o potencial crisis) usando el criterio especificado en la sección de arriba. Informará a su líder para que se active la comunicación al apropiado jefe o líder de la unidad.
- Si el líder de la unidad determina que hay una crisis, se informará a el o a su respaldo designado.
- El Líder o su respaldo informará del evento a otros miembros del equipo central.

6.2.4.2. Organización del Equipo de Trabajo de Administración de Crisis

- El equipo central decidirá si la crisis será manejada por un equipo corporativo o por un equipo de la unidad. Generalmente, crisis las cuales tendrán un impacto sobre toda la Corporación serán manejadas

por un Equipo Corporativo y crisis que afecten únicamente un segmento de la Corporación serán manejadas por el equipo de la Unidad.

- El equipo central es responsable de dirigir las actividades diarias relacionadas con una crisis hasta que esta se asigne a un equipo de una Unidad.

- Si la crisis es para ser manejada por equipo Corporativo, el equipo central designará los miembros del equipo corporativo y asignará responsabilidades específicas teniendo en consideración la naturaleza de la crisis. El equipo central establecerá las políticas finales con respecto a las crisis. El equipo Corporativo será el responsable de implementar las políticas y estrategias establecidas por el Equipo Central e informará al equipo central de toda la información relevante.

- Si el equipo central decide que una crisis específica va ser manejada por un equipo de la unidad, tal equipo deberá mantener informado al equipo Central de sus actividades.

6.2.4.3. Plan de Acción a Implementar / Desarrollo

Se efectúa la recolección y análisis de la Información.

Las personas designadas por el Equipo Central manejarán y reunirán los hechos con respecto a la crisis, incluyendo:

- Que pasó y cuales han sido las respuestas de la Corporación.
- La naturaleza y extensión de algunos heridos o muertos;
- La naturaleza y extensión de algunos daños a los activos de la Corporación;
- La naturaleza y extensión de algunos daños al medio ambiente;
- La causa de la crisis (basado en una investigación profunda); y
- Si sigue existiendo riesgos a clientes, empleados o comunidades afectadas.

Los hechos recolectados con relación a la crisis serán analizados para determinar cual es el problema real y para desarrollar los pasos de acción que encausen el problema y sus causas. Este paso es importante para el éxito administrativo de la crisis.

6.2.4.4. Desarrollo e Implementación del Plan de Respuesta a la Crisis

Un plan específico para responder a la crisis inmediatamente será preparado por el equipo de la unidad el cual es responsable de administrar tal crisis, bajo la dirección del Equipo Central. Este plan de respuesta estará basado en los procedimientos aquí contenidos y en los procedimientos de respuesta aplicable a dicha crisis.

Un plan de respuesta reflejará los siguientes principios:

- ◊ Asuntos prominentes con respecto a consumidores, clientes, empleados y seguridad de la comunidad - LAS PERSONAS SON PRIMERO.

- ◊ Comunicación exacta, completa y oportuna de la información clave para dentro y fuera de la Compañía, con comunicaciones externas manejadas por o coordinadas por Recursos Humanos con autorización de Presidencia. Las comunicaciones deben seguir estos lineamientos:

⇒ Tome la iniciativa - No espere que otros reporten primero; (terceros que no pertenecen a la Compañía)

⇒ Responda a todas las preguntas de los medios rápidamente;

⇒ Corregir objetivamente los malos entendidos que afecten la imagen pública de la compañía;

⇒ Mantener informados a los empleados de la Compañía. antes de anuncios públicos, si es posible y nunca más tarde que los anuncios públicos.

◊ Protección a la reputación de los negocios, activos físicos y la viabilidad de la continuidad económica de la compañía. Una primera meta debe ser retornar a la operación normal a la unidad afectada tan pronto como sea posible mientras se preservan los negocios y las relaciones con los clientes.

* Un plan de respuesta debe ser claro e identificar los objetivos de la Compañía relacionados con resolver la crisis, los nombres y responsabilidades de todas las personas quienes participarán en la respuesta y las acciones requeridas. El equipo de la unidad manejará la implementación del plan de respuesta bajo la supervisión del Equipo Central.

6.2.4.5. Evaluación Posterior a la Crisis

Una evaluación posterior a la crisis de las razones de las crisis y de lo adecuado de la respuesta de la Compañía debe ser hecha para determinar mejorar para el futuro para manejar eventos similares y asegurar que los pasos necesarios para prevenir su recurrencia son tomados.

6.2.5. Responsabilidades de revisión, actualización y entrenamiento

La Presidencia de CLARK S.A. tiene la responsabilidad de designar individuos para:

* Revisar este procedimiento y todos los procedimientos de respuesta al menos anualmente.
* Controlar el entrenamiento continuo de personas que son identificadas en este procedimiento como miembros potenciales del Equipo Corporativo.
* Aconsejar a los líderes de las unidades con respecto a la preparación de los Procedimientos de Respuesta, programas de entrenamiento y planes de respuesta a la crisis y revisión de tales procedimientos, programas y planes de respuesta.
* Controlar el cumplimiento determinado en este procedimiento.

Las personas identificadas en el Apéndice II como responsables de actualización de Procedimientos de Respuesta suministrarán copias de tales Procedimientos de Respuesta actualizados a las personas apropiadas quienes tienen la responsabilidad de revisar tales procedimientos.

El líder de la Unidad asegurará que el plan de respuesta a la crisis para sus unidades de negocios e instalaciones de producción es preparados y actualizados y tendrán el entrenamiento apropiado dentro la compañía.

6.2.6. Procedimientos de respuesta para categorías específicas de crisis.

INTERRUPCIÓN IMPORTANTE DE LA PRODUCCIÓN (FUEGO, EXPLOSIÓN, INUNDACIÓN, DESASTRE NATURAL, ETC.)

Propósito

El propósito de este procedimiento de respuesta es facilitar a los Gerentes de la Unidad intervenir pronta y efectivamente cuando hay interrupción importante en la producción.

Aplicación

Este procedimiento de respuesta aplica a cualquier pérdida inesperada de capacidad de producción o inventario de producto terminado el cual resulte en imposibilidad para producir y/o despachar producto en un período de tiempo significante. Ejemplos de una interrupción importante de la producción son:

- Daño de planta o equipo causado por fuego, explosión, inundación, tornado, falla del equipo, etc., los cuales resultan

en incapacidad para producir/distribuir producto.

- Falla en el proveedor para suministrar una materia prima crítica necesaria para producción de producto.

- Paro nacional de transportadores que resulte en incapacidad para entrega de materias primas y/o distribución de productos terminados.

- Acción legal, paro, o resultado de una decisión para discontinuar las operaciones

Este procedimiento no pretende cubrir reparaciones menores por fallas en equipo, interrupción de la producción por paro de trabajadores cuyo plan de contingencia ha sido desarrollado, o faltantes temporales de la producción resultantes de calidad, salud o seguridad.

Procedimientos adicionales de respuesta pueden ser aplicables dependiendo de la causa de la interrupción (muerte accidental, medio ambiente, amenaza de bomba, etc.). Además, este procedimiento no intenta reemplazar los procedimientos de

emergencia desarrollados para Fuego, terremoto, inundación u otro desastre natural.

Acciones a ser tomadas:

Las siguientes acciones deben ser tomadas inmediatamente en el evento de una interrupción importante en la producción

1. **Notifique a su líder de equipo o gerente de la unidad (dependiendo de la disponibilidad) inmediatamente.**

No permita que un posible evento de crisis no sea reportado por alguna razón. **Si usted identifica interrupción importante de la producción,** usando los ejemplos y el criterio general especificado anteriormente, **usted debe informar a su líder de equipo** de todos los hechos disponibles para fomentar una pronta comunicación (si la situación así lo demanda) al Gerente de la unidad. Si el gerente de la unidad determina que el evento constituye una crisis o crisis potencial, se debe informar al Gerente General

Contener la Crisis de Inmediato

Conjuntamente con las acciones descritas anteriormente y hasta que el administrador de la crisis haya sido asignado y un

plan haya sido desarrollado, **actuar rápida y prudentemente para contener la crisis inmediatamente.** Dependiendo de la naturaleza y seriedad del accidente, usted debe tomar las siguientes acciones:

1. Implemente todos los procedimientos de seguridad de emergencia aplicables para fuego, terremoto, inundación u otro desastre natural, como sea apropiado.
2. Determinar si procedimientos de administración de crisis adicionales deben ser implementados tales cómo muerte accidental o heridas graves, medio ambiente, amenaza de bombas, etc.
3. Establecer la seguridad de los empleados y de la comunidad local y tomar todas las acciones apropiadas para resolver todas las condiciones de inseguridad.
4. Llamar ambulancias y a hospitales si es apropiado
5. Asegurar el sitio accidentado/dañado, el lugar de la planta y establecer la seguridad en el área de producción y unidad.
6. Notificar a las autoridades locales aplicables y a las agencias de administración de emergencias (Departamento de Bomberos, Departamento de Policía, etc.) si es apropiado.

7. Notificar al Departamento de Recursos Humanos para desarrollar plan de comunicaciones.
8. Notificar a Administración de Riesgos
9. Efectuar la primera estimación de los daños en productos terminados o ambientales
10. Notifique al líder del sindicato, si es apropiado.

Definir la Crisis

Una vez la situación inmediata ha sido estabilizada y pendiente de instrucciones adicionales del equipo de administración de crisis, continúe recolectando hechos en un esfuerzo para definir la crisis. Comience una investigación objetiva para determinar la causa del accidente, la naturaleza y extensión de las heridas sufridas y algún daño relacionado con la propiedad y algún otro hecho que considere material para un entendimiento del incidente. Estar preparado para efectuar resúmenes de sus investigaciones al equipo principal. Como parte de su investigación, usted debe:

1. Determinar la naturaleza y extensión de la interrupción.
2. Recoger los nombres, direcciones y números telefónicos de todos los testigos del incidente y todos las otras personas

heridas o de alguna forma comprometidas.

3. Tomar fotografías, hacer dibujos y si es posible, grabaciones de la escena del accidente tan pronto como sea posible.
4. Determine la causa del evento o incidente y liste todas las respuestas tomadas en este momento.
5. Determine la naturaleza y extensión de algunos heridos o muerte.
6. Determine la naturaleza y extensión de algunos daños a los activos de la corporación.
7. Determine la naturaleza y extensión de algún daño al medio ambiente.
8. Determine la naturaleza y extensión de algún daño a la comunidad.
9. Determine el impacto potencial sobre la fuerza de trabajo (reducción de la programación, hacer asignaciones nuevas, plan temporal, etc.)
10. Establecer algún riesgo vigente para los empleados, clientes o comunidad.

Tomar las Siguientes Acciones Adicionales:

1. Comunicar y considerar programar nuevamente todas las

Materias Primas y Productos Terminados.

2. Comunicar la pérdida de producción y/o capacidad de despacho a transportadores y ventas, e indicar las comunicaciones a ser seguidas de despachos y distribución.
3. Considerar las alternativas de fuentes estratégicas.
4. Considerar estrategias de distribución de productos
5. Revise con el Departamento Legal para ver si los contratos con el vendedor o cliente pueden ser violados.
6. Coordinar la estrategia de distribución del producto con Mercadeo, Publicidad y Ventas.
7. Considerar temporalmente la alternativa de planes de espacio para continuar la producción hasta que la reparación o construcción se lleve a cabo.
8. Coordinar el flujo de los servicios públicos con las compañías de servicios para coincidir con la salida de producción.
9. Si es apropiado, desarrollar estrategias para retornar la planta y el equipo a su operación normal.
10. Considerar opciones para modificar y convertir equipos alternos que reúnan las demandas de producción.
11. Indicar fuentes alternas de capacidad de producción. (Internacional, Contratos externos Etc.)
12. Considerar la identificación y cancelación de activos.

13. Si es apropiado, coordinar la terminación y presentación de los papeles de trabajo del reclamo de seguros.

Revisión de la Crisis

Revise la efectividad de este procedimiento y todos los sistemas y recursos utilizados en el manejo de la crisis. Identifique cambios que deben efectuar y otras acciones correctivas.

1. Que tan efectivos fueron los procedimientos de contención, definición y respuesta a la crisis?
2. Como fue la respuesta y la disponibilidad de los recursos claves cuando fueron llamados para soportar los esfuerzos de administración de crisis?
3. Que tan efectivo fue el equipo de la crisis para responder la crisis?
4. Qué consejo adicional es necesario para los individuos afectados por la crisis?

CONTACTOS CLAVES.

Departamento de Policía	101
Departamento de Bomberos	102
Hospital	911
Ambulancia	911

RELACIONES CON EMPLEADOS (HUELGAS, PARADAS DE TRABAJO, ETC)

Propósito

El propósito de este procedimiento de respuesta es facilitar a los Gerentes de la Unidad intervenir pronta y efectivamente con un evento de crisis de relación con empleados.

Aplicación

Este procedimiento de respuesta aplica a cualquier problema de relación con empleados que pueden afectar seriamente a la compañía para cumplir sus objetivos de seguridad de los activos y empleados, financieros, producción y servicio al cliente. Ejemplos de eventos de crisis de relaciones con empleados son:

Una huelga iniciada en una unidad sindicalizada en conjunto con el convenio normal de obligaciones.

Una parada en la unidad sindicalizada o no iniciada por empleados en protesta por algunas acciones administrativas o en un intento por forzar un punto de vista.

La potencial seriedad de tales eventos debe ser evaluada en términos de potenciales efectos adversos sobre la seguridad de los empleados, producción, servicio al cliente, finanzas corporativas y presiones y reacciones públicas.

Procedimientos adicionales de respuesta pueden ser aplicables dependiendo de la causa o efecto del evento (interrupción importante de la producción, publicidad adversa, etc.). Además, este procedimiento no intenta reemplazar y planes detallados para huelgas que hayan sido desarrollados por la administración del sindicato de la unidad con guías del Departamento de Recursos Humanos y Departamento Legal. Más bien este procedimiento intenta establecer esfuerzos para respuestas iniciales para todos los eventos de crisis en relaciones con empleados.

Acciones a ser tomadas:

Las siguientes acciones deben ser tomadas inmediatamente en el evento de una interrupción importante en la producción.

1. Notifique a su líder de equipo o gerente de la unidad (dependiendo de la disponibilidad) inmediatamente.

No permita que potencial evento de crisis no sea reportado por alguna razón. **Si usted identifica interrupción importante de la producción,** usando los ejemplos y el criterio general especificado anteriormente, **usted debe informar a su líder de equipo** de todos los hechos disponibles para fomentar una pronta comunicación (si la situación así lo demanda) al Gerente de la unidad. Si el gerente de la unidad determina que el evento constituye una crisis o crisis potencial, se debe informar al Gerente General

Contener la Crisis de Inmediato

Después de notificar apropiadamente el evento de crisis del medio ambiente y hasta que el administrador de la crisis haya sido asignado y un plan haya sido desarrollado, **actuar rápida y prudentemente para contener la crisis inmediatamente.** Dependiendo de la naturaleza y seriedad del problema, usted debe tomar las siguientes acciones:

Determinar si procedimientos adicionales de administración de crisis deben ser implementados tal cómo interrupción importante de la producción, publicidad adversa, etc.

Instituir las condiciones del plan de huelga de la unidad, si es aplicable

Contactar todos los empleados y motivarlos/persuadirlos para que continúen trabajando, si es pertinente.

Empezar una investigación para conocer las causas de la crisis de relación con empleados, y averiguar soluciones que serán necesarias para disminuir la operación como económica y seguramente sea posible.

Notificar a recursos humanos corporativos

Notificar al Departamento Legal

Notificar a seguridad corporativa, discutir y desarrollar planes que pueden ser la mejor protección para los empleados, equipo e instalaciones de la Compañía.

Notificar al Departamento de Policía local de la situación y una posible necesidad de asistencia.

Definir la Crisis

Una vez la situación inmediata ha sido estabilizada y pendiente de instrucciones adicionales del equipo de administración de crisis, continúe recolectando hechos en un esfuerzo para definir la crisis. Comience una investigación objetiva para determinar la causa del problema, la naturaleza y extensión de las heridas sufridas y algún daño relacionado con la propiedad y algún otro hecho que considere material para un entendimiento del incidente. Estar preparado para efectuar resúmenes de sus investigaciones al equipo principal. Como parte de su investigación, usted debe:

Determinar la naturaleza, extensión y causa de la crisis de relación con empleados, compile y actualice continuamente un registro o resumen objetivo y cronológico del evento de crisis, incluyendo todas las respuestas de la compañía a la crisis.

Si es aplicable prepare listas identificando todos los empleados envueltos en la huelga, parada de trabajo, también como aquellos empleados no envueltos en la crisis de relación con empleados.

Si es aplicable, compile una lista de los nombres y direcciones de todos los líderes sindicales locales e internacionales.

Si es posible, averiguar la lista “prioridad de demandas de los líderes de los empleados envueltos en el evento (líderes del sindicato, si es aplicable).

Determine el impacto potencial sobre la fuerza de trabajo (reducción de la programación, hacer asignaciones nuevas, plan temporal, fuentes alternas de producción etc.)

Tomar las siguientes acciones adicionales:

- Establecer un comando central y comunicaciones continuas entre el personal del sitio y el equipo de administración de crisis.
- Si es apropiado, desarrolle y suministre toda la información necesaria para Recursos Humanos para posible emisión de pronunciamientos.
- Mantener un archivo central de todos los papeles de trabajo y otros registros relacionados con los eventos de la crisis.
- Desarrollar un plan para salvar los ingresos y egresos

de la localidad, acomodando empleados temporalmente, proveedores, contratistas externos, empleados no comprometidos y administración.

- Considerar que la producción y servicio al cliente son los más esenciales y hacer recomendaciones para su Jefe de sector/unidad de servicio en cuanto tales productos y servicios deben continuar sin interrupción.
- Comunicar pérdida potencial de la producción y/o capacidad de despachos para transporte y ventas.
- Trabajar con el Dpto. Legal, Considerar la necesidad de identificar y contactar consejeros legales locales externos.
- Reportes de progreso sobre todas las investigaciones al equipo de administración de crisis

Revisión de la Crisis

Revise la efectividad de este procedimiento y todos los sistemas y recursos utilizados en el manejo de la crisis. Identifique cambios que deben efectuar y otras acciones correctivas.

Que tan efectivos fueron los procedimientos de contención, definición y respuesta a la crisis?

Como fue la respuesta y la disponibilidad de los recursos claves cuando fueron llamados para soportar los esfuerzos de administración de crisis?

Que tan efectivo fue el equipo de la crisis para responder la crisis?

Qué consejo adicional es necesario para los individuos afectados por la crisis?

Contactos Claves

Departamento de Policía	101
Departamento de Bomberos	102
Hospital	911
Ambulancia	911

AVERÍA DEL COMPUTADOR O SABOTAJE

Propósito

El propósito de este procedimiento de respuesta es facilitar a los Gerentes de la Unidad intervenir pronta y efectivamente cuando hay eventos de sabotaje y fallas de la computadora

Aplicación

Este procedimiento de respuesta aplica a cualquier situación que pueda originar daños físicos o pérdida del procesamiento computarizado de algún período. La falla puede resultar de una pérdida del funcionamiento del procesamiento, la inhabilidad para obtener acceso a la computadora o una falla externa resultante de la inhabilidad para procesar información en un período de tiempo. Los siguientes ejemplos son eventos de fallas de la computadora:

Una explosión en las instalaciones de la computadora que impiden las operaciones de la unidad.

Se dañan las comunicaciones que suministran servicio a una porción importante de la red de datos.

Los archivos de datos son saboteados por un hacker dando información no confiable.

Procedimientos adicionales de respuesta pueden ser aplicables dependiendo de la causa o efecto del evento. Cada instalación computarizada de CLARK S.A. debe mantener un plan de continuidad de los negocios, incorporando procedimientos de

recuperación de emergencias para restaurar las funciones de procesamiento de la computadora Además, este procedimiento no intenta reemplazar los procedimientos o planes desarrollados para restaurar el proceso de computadora, en el evento de una falla en la computadora.

Acciones a ser tomadas:

Las siguientes acciones deben ser tomadas en el evento de un sabotaje o falla en la computadora.

Notificar inmediatamente a su supervisor o Jefe de Sector/Unidad de Servicio

No permita que un posible evento de crisis se quede sin reportar por alguna razón. Si usted identifica un evento de falla en la computadora, usando los ejemplos y criterio especificado anteriormente debe informar inmediatamente al Gerente de la unidad y a seguridad corporativa de todos los detalles disponibles. Si el gerente de la unidad determina que el evento constituye una crisis o crisis potencial, se debe informar al Gerente General.

Contener la Crisis Inmediatamente

Después de notificar apropiadamente la falla de la computadora o sabotaje y hasta que el administrador de la crisis haya sido asignado y un plan haya sido desarrollado, **actuar rápida y prudentemente para contener la crisis inmediatamente.** Dependiendo de la naturaleza y seriedad del evento, usted debe tomar las siguientes acciones:

Establezca la seguridad de los empleados y de la comunidad local y tome las acciones apropiadas para resolver las condiciones inseguras.

Llame a las ambulancias, hospitales, y agencias de administración de emergencias (Departamento de Bomberos, Policía, etc.) si es apropiado.

Seguridad en las instalaciones computarizadas dañadas.

Determine si procedimientos adicionales de administración de crisis necesitan ser implementados tales como muerte accidental o heridos graves, interrupción importante de la producción, amenaza de bomba, etc.

Notifique a Recursos Humanos para desarrollar un plan de comunicaciones. Refiera alguna averiguación de los medios a Recursos Humanos.

Notifique a mantenimiento/ingeniería de la unidad para que establezca el daño en las instalaciones de la computadora

Nombre un administrador para coordinar la recuperación de las operaciones computarizadas y el plan de Continuidad de los Negocios.

Notifique a los miembros del equipo definidos en el Plan de Continuidad de los negocios para asistir en la recuperación de las instalaciones de la computadora y comunicaciones en red.

Notifique a administración de riesgos

Definir la crisis

Una vez la situación inmediata ha sido estabilizada y pendiente de instrucciones adicionales del equipo de administración de crisis, continúe recolectando hechos en un esfuerzo para definir la crisis. Comience una investigación objetiva para determinar la causa del evento, la naturaleza de algún daño en la

propiedad y algún otro hecho que considere material para un entendimiento del incidente. Estar preparado para efectuar resúmenes de sus investigaciones al equipo principal. Como parte de su investigación, usted debe:

Determine la naturaleza y extensión de algunos heridos o muerto

Recoger los nombres, direcciones y números telefónicos de todos los testigos del incidente y todas las otras personas heridas o de alguna forma comprometidas.

Tomar fotografías, hacer dibujos y si es posible, filmaciones de las áreas y equipos afectados.

Determine la naturaleza y extensión de algún daño al equipo computarizado y las comunicaciones en red.

Determine la causa del evento o incidente y liste todas las respuestas tomadas en este momento.

Determine el impacto potencial sobre los empleados.

Determine la naturaleza y extensión de algún daño al medio ambiente

Determine la naturaleza y extensión de algún daño a la comunidad

Establecer algún riesgo vigente para los empleados o la comunidad.

Tomar las siguientes acciones adicionales:

- Considerar la estrategia de procesamiento en un computador alterno para continuar con la actualización de las operaciones.
- Notificar al proveedor local de una situación de desastre.
- Recobrar la información de respaldo almacenada en un lugar fuera del sitio
- Considerar un mensaje para llamadas de ayuda de escritorio para comunicar a todos los usuarios de computadores el progreso de la recuperación.
- Notificar a los usuarios propietarios de aplicaciones críticas de negocios sobre el progreso de un proceso

de recuperación de desastres.

- Considerar el establecimiento de un Centro de Control de Emergencia para coordinar y monitorear el proceso de recuperación.
- Considerar una oficina alterna para continuar recuperando las operaciones computarizadas.
- Coordinar el flujo de servicios públicos (electricidad, teléfono, etc.) con las empresas públicas, para que coincida con la recuperación de las operaciones del computador
- Considerar la identificación de activos y cancelarlos
- Coordinar la restauración de los equipos de cómputo destruidos.

Revisión de la Crisis

Revise la efectividad de este procedimiento y todos los sistemas y recursos utilizados en el manejo de la crisis. Identifique cambios que deben efectuar y otras acciones correctivas.

Que tan efectivos fueron los procedimientos de contención, definición y respuesta a la crisis?

Como fue la respuesta y la disponibilidad de los recursos claves cuando fueron llamados para soportar los esfuerzos de administración de crisis?

Que tan efectivo fue el equipo de la crisis para responder la crisis?

Qué consejo adicional es necesario para los individuos afectados por la crisis?

Qué medidas deben ser incluidas en un plan de prevención para asegurar que no ocurrirá otro incidente?

Que información debe ser comunicada a otras unidades computarizadas de CLARK S.A. que pueden potencialmente tener situaciones similares?

Contactos Claves:

Departamento de Policía	101
Departamento de Bomberos	102
Hospital	911
Ambulancia	911

CAPÍTULO VII

7. PLAN DE CONTINGENCIA

7.1. ESTRUCTURA DEL PLAN

Durante las operaciones normales de negocio existe la probabilidad de pérdidas potenciales o interrupciones no programadas asociadas con un desastre o contingencia mayor, por lo que es importante el desarrollo de un plan viable y factible de recuperación que asegure la continuidad de las operaciones de la Compañía.

El planeamiento adecuado, la preparación, y la comunicación son los ingredientes necesarios para un exitoso plan de recuperación en caso de contingencia o desastre.

En el caso de una situación de contingencia o desastre, es importante disponer de una estrategia de recuperación que pueda proveer el reinicio del negocio en un tiempo razonable y predeterminado. Por lo tanto, la importancia de un Plan de contingencias y recuperación en caso de desastres es vital.

El presente documento ilustra los posibles tipos de contingencias y desastres, y los planes de acción para la recuperación de la información y la continuidad del negocio de la oficina principal.

Definición de contingencia

Una contingencia se define como cualquier evento no planeado que hace que las actividades de negocio no sean operadas normalmente durante un determinado periodo de tiempo, para la cual existe una solución que permite la recuperación en un tiempo razonable.

Las contingencias comunes se deben normalmente a los eventos como:

1. Falla de la red en una localidad.
2. Falla en los enlaces de telecomunicaciones entre localidades.
3. Falta de suministro de corriente eléctrica.
4. Fallas humanas en la operación de la red o equipos de cómputo.

Esto implica que deben existir equipos de repuesto, redes de datos alternas o suministro in-interrumpido de fluido eléctrico para minimizar el impacto de una contingencia. El plan de recuperación en caso de contingencia o desastre considera el disponer de mecanismos para reanudar las actividades de negocio mientras exista dicha contingencia.

También hay que indicar que todos los servicios de aplicaciones y las bases de datos que soportan SAP R/3, por lo que hay una alta dependencia en las telecomunicaciones para acceder a estos servicios. Mantener y soportar la disponibilidad de las telecomunicaciones en Ecuador se convierte en una actividad vital que asegura la continuidad de las operaciones de negocio de manera normal.

Definición de desastre

Un desastre se define como cualquier evento no planeado que hace un lugar inoperable o inaccesible. Diversos tipos de desastre pueden ocurrir y varían de:

1. Comunes:
    - Fallos masivos.
    - Daños accidentales.

2. Extraordinarios:
    - Robo.
    - Destrucción del centro de cómputo.
    - Incendio.
    - Guerra.
    - Atentado Terrorista.

3. Naturales:
    - Terremoto.
    - Inundación.
    - Huracán.
    - Nevadas intensas.
    - Erupción volcánica.
    - Tormentas eléctricas.

Los desastres naturales y extraordinarios no serán considerados en este plan ya que estos ameritan procedimientos incluidos en el "Manual de Administración de Crisis" de CLARK S.A.

El presente plan de contingencias y recuperación en caso de desastre considerará los siguientes desastres:

- Tormentas eléctricas que destruyan parcial o totalmente la red de datos.
- Fallas físicas en la red de datos y o comunicaciones.

Dichos eventos pueden ocurrir tanto en localidades de CLARK S.A. Andino. Los efectos de estas situaciones hacen importante el mantener la continuidad del negocio cuando SAP R/3 este parcial o totalmente no disponible.

Localidades físicas y ambiente de trabajo

La Cía Clark S.A. se compone de varias localidades separadas geográficamente de las cuales la oficina principal de Ecuador hace parte de ellas.

OBJETIVOS

Los objetivos del plan de recuperación en caso de desastre incluyen, pero no están restringidos a:

- Minimizar los efectos de una contingencia o desastre en las funciones críticas al proveer de un conjunto de procedimientos y tareas a ser usados en el evento.
- Responder a una situación de contingencia o desastre rápida y efectivamente.
- Reunir al personal necesario para reactivar el proceso con las interrupciones menores respecto al servicio al cliente.
- Restauración por fases en el tiempo de todas las aplicaciones y servicios posteriormente a la interrupción a causa de la contingencia o desastre.

Este plan busca minimizar:

- El número de decisiones que deben ser hechas después de una contingencia o desastre.
- La necesidad de desarrollar, probar, y corregir nuevos procedimientos durante el desastre.
- Depender de la participación de cualquier persona específica o grupo de personas durante el proceso de recuperación.
- El período de tiempo tomado para el proceso de recuperación.
- Las pérdidas asociadas con la interrupción de las actividades del negocio.
- La confusión y la exposición a errores.
- La duplicación de esfuerzos.

El alcance de estos objetivos asegurará la estabilidad operacional a través de un proceso de recuperación.

ENUNCIADO DE LA POLITICA

Se reconoce la importancia de establecer métodos que permitan a los usuarios internos, mantener la continuidad del negocio y proveer el servicio a nuestros clientes en el evento de una contingencia o desastre en alguna de las localidades de CLARK S.A.

Es la política del Departamento de Sistemas, mantener un “Plan de Contingencias y Recuperación en Caso de Desastres” viable operativa y económicamente, para soportar el restablecimiento de las operaciones de servicio en el evento de una interrupción.

El Plan de Contingencias y Recuperación en Caso de Desastre ha sido desarrollado para alcanzar los estándares corporativos de CLARK S.A. con base en el CFI No. 07-01, Apéndice K - Sistemas de Información. Operaciones exitosas de recuperación dependen de los siguientes puntos:

- Llevar a cabo pruebas amplias del plan.
- Modificar el plan con base en las pruebas hechas.
- Mantener un plan actualizado.
- Brindar entrenamiento al personal asignado en las diferentes secciones del plan.
- Soporte para el “Crisis Management” de CLARK Corporation.

ALCANCES

Este plan no es un plan completo para todas las operaciones de CLARK S.A. No documenta las acciones específicas de los departamentos del negocio o una estrategia de recuperación global corporativa. Otros planes de recuperación y los procedimientos

correspondientes respecto a recuperación en caso de desastre son responsabilidad de los departamentos específicos.

El plan considera los siguientes aspectos:

- Reestablecimiento de los equipos y enlaces de telecomunicaciones vitales para la operación del negocio.
- Reestablecimiento de las áreas vitales de la red de computadoras.

El plan no considera los siguientes aspectos:

1. Emergencias de edificios y procedimientos de evacuación.
2. Valoración de riesgos en los edificios.
3. Evaluación y declaración de desastres en edificios.
4. Recuperación de las diferentes unidades y departamentos de la Compañía.
5. Equipos no relacionados con la red de datos (PBX, máquinas de fax, fotocopiadoras, etc.)
6. La red de telecomunicaciones de Corporación.
7. Operaciones relacionadas con el TCC de Corporación.

PREMISAS

Los siguientes supuestos fueron hechos al desarrollar el plan:

1. El TCC de CLARK S.A. Corporation en USA es responsable de:

   - Mantener copias actualizadas de respaldo de todos los archivos y programas apropiados en un lugar fuera de la Compañía. En este plan no se establece este procedimiento, pues se asume que existe.
   - Restaurar los archivos y software más actualizado residentes en el lugar de respaldo fuera de la compañía.
   - Soportar el acceso a la red global total o parcialmente en eventos extraordinarios o desastres naturales ocurridos en la localidad donde opera el TCC.
   - Mantener un Plan de Contingencias y Recuperación de Desastres actualizado para el TCC.

2. El Departamento de Sistemas de Información es responsable de:

   - Soportar el acceso local a la red global de datos.
   - Soportar el acceso a la red de datos andina y las redes locales de cada uno de los países.

- Mantener un Plan de Contingencias y Recuperación en caso de *Desastre* local actualizado.
- Mantener contratos con proveedores conforme se requiera.
- Entrenar al personal clave para llevar a cabo las funciones definidas dentro del plan.
- Notificar a los usuarios de aplicaciones críticas que se está en una situación de contingencia o desastre.
- Participar en las acciones definidas en el *"Crisis Management"* de CLARK S.A. cuando sea notificado.

3. El plan supone que:

- El edificio del TCC donde se encuentran los servidores de aplicaciones y datos principales, y su red de datos no han sido destruidos o se encuentran inaccesibles para el personal. En caso contrario, el "Crisis Management" prevé soluciones al respecto, lo mismo que el plan desarrollado por el TCC.

- La situación de contingencia o desastre ocurrirá en el peor tiempo posible.

- Las cajas de seguridad -dispuestas por el TCC- situadas fuera de la compañía y los materiales que contiene, no han sido afectados por el desastre o por características de la misma.

- Secciones del plan global podrán ser utilizadas para recuperación de interrupciones menores.

- Desastres de escala nacional estarán considerados dentro del plan, siempre y cuando el desastre no afecte a los servicios vitales de la compañía como: Imposibilidad de obtener suministro de electricidad, daño total en las instalaciones, etc.

- Los respaldos han sido hechos correctamente por el TCC y los medios magnéticos en los cuales se encuentran pueden ser leídos.

- Existen mecanismos para proporcionar infraestructuras alternas de emergencia tales como plantas eléctricas, equipo y red de datos y telecomunicaciones de emergencia.

- Establecimiento de alianzas con proveedores críticos para el funcionamiento de toda la infraestructura de telecomunicaciones y datos.

7.2. PROCEDIMIENTO PARA ATENCIÓN DE FALLAS EN INFRAESTRUCTURA

✓ Conexión física a la red local

Tabla 7.1: Análisis de la Conexión Física

Problema:	No hay acceso a la red de datos.
Acción:	1. Determinar si el usuario está conectado a la red. 2. Corregir problemas de nivel físico, conectores, LAN Jack, Switch. 3. Si se determina que el problema es una avería que va a ser resuelta por más de 6 horas, habilitar puntos de red de emergencia.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

✓ Acceso al Enterprise Network

Tabla 7.2: Análisis del Enterprise Network

Problema:	No hay acceso al Global Desktop.
Acción:	1. Revisar entorno de red. 2. Si no hay acceso al GDXP, reportar enlace al proveedor local. 3. Si la falla y/o resolución del problema se demora más de 6 horas comunicar a usuarios claves el acceso alternativo vía RAS 4. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Acceso al File&Print Server**

Tabla 7.3: Análisis de las Impresoras

Problema:	Problema no se puede imprimir o acceder archivos en el servidor.
Acción:	1. Revisar acceso tipo share. 2. Revisar si puede imprimir desde Windows. 3. Revisar los servicios del servidor. 4. Contactar a "Help-Desk" MIS Local. 5. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

- ✓ **Acceso al Correo Electrónico**

Tabla 7.4: Análisis de Acceso al e-mail

Problema:	No hay acceso al correo electrónico.
Acción:	1. Revisar si hay acceso al Address Book. 2. Enviar y/o recibir correo. 3. Si no se pueden realizar las acciones anteriores, contactar al Help Desk de MIS Local. 4. Si se determina que el problema es en KCC, contactar al responsable en KCC.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

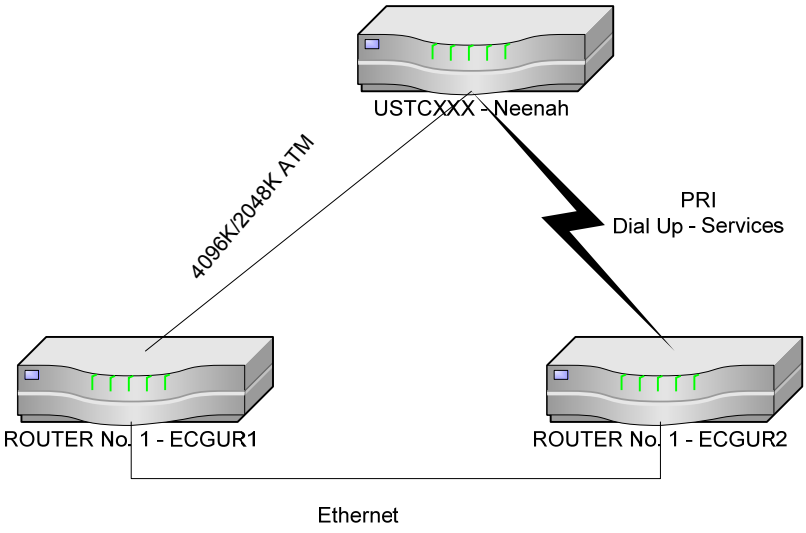
Errores en comunicación de datos

- ✓ **Esquema de comunicaciones**

Comunicaciones Oficina Principal Ecuador con TCC

Dentro de este grupo se encuentran los enlaces de comunicaciones de datos considerados centro de comunicaciones en el TCC en USA

Gráfico 7.1: Comunicación Ecuador – Neenah – USA



Fuente: Cía Clark S.A

✓ **Enlace Internacional**

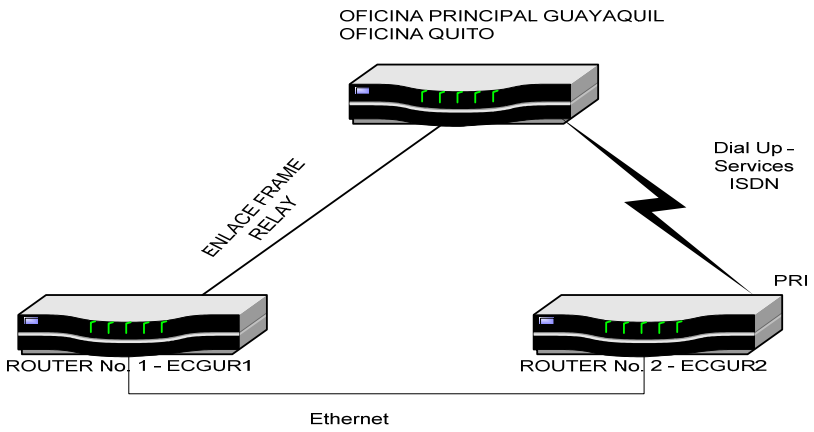
En la actualidad existe un enlace con capacidad 4096K/2048K por donde fluye el trafico de la red hacia la corporación y en condiciones normales.

Para la contingencia existe un servicio de RAS que se conecta de manera automática con el TCC cada vez que falla la conexión internacional.

✓ **Enlaces ISDN De Contingencia Oficina Locales**

Planta Mapasingue, Oficina de Distribución Quito se utilizan líneas ISDN/RDSI en cada sitio, que hacen conexión al sitio central en Guayaquil; cuando un enlace Frame Relay falla el sistema marcara automáticamente al sitio principal.

Gráfico 7.2: Enlace Local



Fuente: Cía Clark S.A

En la Oficina de Quito, existe un segundo circuito redundante que opera como contingencia en caso de falla del primero, la contingencia es activada de forma automática cuando el enlace primario falla. Los demás sitios deben utilizar el acceso RAS por línea conmutada o banda ancha.

- ✓ **Resumen Enlaces – Contingencia**

Tabla 7.5: Enlaces - Contingencia

SITIO	ENLACE	CONTINGENCIA
Oficina Quito	Frame Relay – 34000K	ISDN
Of. Distribución	Banda Ancha – 350K	Acceso RAS
Of. Ventas	Frame Relay – 1024K	Acceso RAS
Bodega de Productos	Frame Relay – 2048	Enlace redundante
Bodega de Fibra	Frame Relay – 2048	Enlace Redundante

CAPÍTULO VIII

8. PRUEBA DEL PLAN DE CONTINGENCIA

8.1. ANTECEDENTES

Nombre del Plan: Plan de Continuidad de Negocios.

Fecha Ejercicio: Enero de 2009

Localidad: Oficinas de Clark S.A.

Participantes: Dpto. ITS

Acciones a seguir:

- ✓ Aplicaciones del negocio

1. Preparar y documentar carta de aceptación de aplicaciones.
2. Terminar documentación de recuperación de aplicación mantenimiento de planta.

- ✓ Estrategia de Continuidad de Negocio

1. Completar información de los IDFs.
2. Actualizar información en el sitio de administración de red corporativa.
3. Obtener y confirmar información de redes inteligentes para equipos de comunicaciones.

4. Confirmar revisión y aprobación de procedimientos de recuperación y plan de continuidad de negocios con el LAO grupo de servicios computarizados.

✓ Almacenamiento respaldos fuera de las oficinas

1. Mejorar el lugar de almacenamiento y rotulado de respaldos diarios.
2. Confirmar que el respaldo de información vital para el negocio se esté almacenando adecuadamente.

✓ Actividades de respuesta

1. Agregar números telefónicos de casas de habitación en la lista de contactos.
2. Incluir lista de chequeo de tareas en el Procedimiento de Recuperación en caso de Desastre.

✓ Actividades de reanudación

1. Los números de teléfono de las casas del personal de ITS necesitan ser incluidos.
2. Coordinar con LAO servicios computarizados y la red para la creación de una estrategia de recuperación definida para la restauración de enrutadores y switches.

✓ Consideraciones Generales

1. Almacenar copias del plan en sitios autorizados fuera de las Oficinas de Clark S.A.

✓ Procedimientos de Referencia Externos

1. Verificar la existencia del procedimiento de Control Interno en las Oficinas de Clark S.A.
2. Verificar la existencia de un Manual de Emergencias para las Oficinas de Clark S.A.

✓ Capacitaciones periódicas al personal

1. Informar acerca de la existencia del manual de contingencia.
2. Capacitación constante (cada trimestre) al personal sobre evacuaciones y seguridad.
3. Incentivar al personal e informar mediante folletos, volantes, evacuaciones y evaluaciones sobre que hacer en caso de desastres.

8.2. PRUEBAS Y VERIFICACIÓN DE LA LISTA DE CHEQUEO

Aplicaciones del Negocio:

Verifique que las aplicaciones de negocio están documentadas para cada plataforma computacional de la planta, y que cada aplicación haya sido identificada como crítica o no crítica.

Asegúrese que los nombres de ITS y usuarios dueños y responsable de cada aplicación estén identificados y correctos.

Comentarios: Todas las aplicaciones están incluidas e identificadas como críticas ó no críticas.

Verifique que cartas de aceptación del usuario hayan sido desarrolladas para cada aplicación.

Verifique que se hayan desarrollado Planes de Recuperación en Caso de Desastre.

Comentarios: Se encontraron Procedimientos de Recuperación en caso de desastres para las siguientes aplicaciones:

- ✓ Nómina – Adam
- ✓ Mantenimiento Planta – MMS: Existe un procedimiento parcial que debe ser terminado.
- ✓ Fuerza de Ventas – Sysgold

Verifique que las copias de las cartas de aceptación del usuario y los Procedimientos de Recuperación en Caso de Desastre hayan sido enviadas al Coordinador Corporativo de Continuidad del Negocio.

Estrategia de Continuidad del Negocio

Verifique que las especificaciones técnicas de los servidores estén correctas.

Comentarios: Los servidores están apropiadamente incluidos.

Verifique que la información de comunicaciones de datos esté correcta (MDF and IDF's)

Comentarios: Existe una adecuada documentación del MDF en el.

Verifique que los Diagramas de Red estén actualizados con los que tiene la administración corporativa de red.

Comentarios: La información si está actualizada.

Asegúrese que todo el equipo de repuesto necesitado en la planta ha sido identificado y almacenado en una localidad segura.

Los contratos SMARTNETS de enrutadores y switches principales están activos con cada uno de los Proveedores.

Verifique que las estrategias de cambio de hardware (Ej.: equipo de repuesto, suministrado por el proveedor, equipo redundante, sitio alterno, etc.) haya sido identificado para restaurar las aplicaciones

dentro de las expectativas de tiempo y costo, con mínimo riesgo para la planta.

Comentarios: Los contratos de servidores con la compañía SONDA DEL ECUADOR permiten reemplazar partes y servidores, de acuerdo al contrato establecido.

Se tiene un contrato de redes inteligentes para enrutadores y switches principales con el proveedor Emtelco.

Asegúrese que todo el personal (Ej., de ITS, proveedores, cliente, etc.) involucrados con las estrategias de hardware son concientes de sus responsabilidades.

Comentarios: Las estrategias de recuperación de servidores y equipos de telecomunicaciones están a cargo del LAN Admin y del ITS Manager.

Verifique que las estrategias de recuperación han sido aprobadas por la administración y LAO servicios computarizados.

Respaldos fuera de las oficinas

Asegúrese que la Valoración del Riesgo para la planta esté documentada.

Comentarios: La Valoración del Riesgo se realizó en Mayo 2008 y está documentado.

Verifique que los respaldos están siendo realizados y estén documentados.

Comentarios: El procedimiento ITS define la estrategia de respaldo. En el se identifican los mecanismos de revisión de los respaldos, periodicidad y almacenamiento (revisar lugar, rotulado, documentación de respaldo diario).

Verifique que los suministros necesitados para la recuperación estén documentados.

Comentarios: ITS no es responsable de la provisión de suministros en las oficinas de Quito.

Verifique que los registros vitales necesarios para la recuperación estén documentados.

Verifique que el lugar en donde se almacenan los respaldos está a una distancia aceptable no sujeta a los mismos riesgos que la localidad primaria y esté documentado.

Comentarios: Los respaldos semanales y mensuales son guardados en las instalaciones del Banco Bolivariano localizados a 15 KM de las oficinas de Clark S.A.

Verifique que los procedimientos de respaldo estén documentados.

Comentarios: La estrategia de respaldo está documentada en el procedimiento ITS, el cual puede ser accedido en la Intranet de Clark S.A.

Actividades de respuesta

Revise la lista de Contactos y verifique los nombres y números de teléfono del personal que será llamado para responder a la situación de desastre.

Verifique los nombres del personal que puede declarar una situación de desastre.

Comentarios: El desastre puede ser declarado por el ITS Manager ó el LAN Admin.

Asegúrese que existan tareas y procedimientos para responder a una situación de desastre.

Actividades de Reanudación

Revise la lista de contactos y verifique que los nombres y teléfonos de los empleados, proveedores y clientes puedan ser llamados para recobrar el ambiente e infraestructura computacional.

Asegúrese que los procedimientos de notificación, transporte y de contratos estén debidamente documentados.

Asegúrese que las tareas, procedimientos de soporte técnico, y/o manual existan para recobrar el quipo computacional e infraestructura de soporte.

Consideración General

Verifique que la gente responsable de responder y recuperar el procesamiento computacional o la infraestructura de soporte tengan acceso a copias del plan fuera de las oficinas.

Verifique que una copia del plan esté guardada en un sitio fuera de las instalaciones principales.

Referencias a Procedimientos Externos

Asegúrese que el plan es compatible con los Controles Internos de la planta.

Asegúrese que el plan esté referenciado o sea compatible con el Manual de Emergencia de la planta.

8.2.1. Verificación de las Aplicaciones

Suposiciones

Hay una serie de suposiciones hechas por cada dueño de Aplicación para recuperar totalmente una Aplicación, que asume

que ITS cuenta con una serie de Procedimientos para resolver la Recuperación de los componentes de una Aplicación. (Agregar o remover suposiciones según requerido):

- Equipo de Continuidad de Negocio: Provee el Procedimiento para la Recuperación de la Aplicación en el caso de un Desastres.
- Equipo de Seguridad al Sistema: Recuperar la seguridad de la Aplicación y los grupos de seguridad de administración de redes, utilizando los Procedimientos establecidos para Recuperación en caso de Desastres de seguridad de los sistemas.
- Grupo de administración de servicios Corporativos: Recuperar o reconstruir los servidores de la Aplicación con todo el software y hardware necesario, además de los componentes del activo utilizando los Procedimientos de Recuperación en caso de Desastres.
- Equipo de administración de la base de datos: Recuperar las bases de datos de la Aplicación utilizando los Procedimientos para la Recuperación en caso de Desastres.
- Administración, Web-Notes, Internet: Recuperar, recobrar o reconstruir componentes específicos de la Aplicación utilizando los Procedimientos de Recuperación en caso de Desastre del grupo Web-Notes/Intranet.

Participantes del Test:

Para cada elemento de la lista de chequeo, identifique cual equipo es responsable de proveer información sobre la pregunta.

Tabla 8.1: Test de Chequeo de Aplicaciones

Lista de Chequeo	Comentarios
Contacto del personal	
Está actualizada la lista de contactos de ITS en q*uien corrige* la Aplicación?	Si
Los miembros del grupo de ITS responsables de la Aplicación conocen como utilizar y actualizar el *Quien corrige (Whofixes)*?	Si.
Tiene el equipo de ITS de la Aplicación una lista actualizada de como contactar a los actuales usuarios y números de teléfono para cualquier usuario que necesite ser localizado, para darle soporte a la Recuperación de la Aplicación? Si la respuesta es si, en donde están almacenados la lista de contactos y los teléfonos?	Si, se encuentra en la carpeta COBTFN01\Share\Santillana\MIS\Desarrollos\Sysgold\ La lista de Contactos se encuentra al final del procedimiento: http://cosaaw01.kcc.com/Auditoria/PROCEDIMIENTOS/index.htm Procedimiento ITS – 023.
Quién tiene acceso a lista de contactos de usuarios?	Carlos Londoño. Líder ITS
Tiene el equipo de ITS de la Aplicación una lista actualizada de como contactar cualquiera de los clientes externos y/o proveedores que sean necesario localizar, si ocurre un desastre? Si la respuesta es si, en donde están almacenados la lista de contactos y los teléfonos?	Si, existe. Referencia Plan de Continuidad del Negocio.
Quién tiene acceso a la lista de clientes y proveedores?	Carlos Pelaez, Jaime Valderrama, Adriana Gomez.
Está el equipo de ITS de la Aplicación seguro de que Procedimiento de Recuperación en caso de Desastres de la Aplicación provee suficiente detalle de cuáles grupo de servicios del sistema deben ser contactados?	Si.

Tabla 8.1: Test de Chequeo de Aplicaciones (Continuación)

Lista de Chequeo	Comentarios
Carta de aprobación del usuario	
Está la carta de aprobación del usuario actualizada y en concordancia con el nombre(s) incluido en el reporte Bi-mensual de Recuperación en caso de Desastres de la Aplicación emitido por el Coordinador Corporativo de *Business Continuity*? Si no, cuando se obtendrá una nueva carta de firmas.	Ya se encuentra creada y firmada.
En donde se almacena la carta de aprobación del usuario? (Se necesitan versiones electrónicas e impresas).	Carlos Londoño tiene la copia impresa. La electrónica está en el directorio COBTFN01\Share\Santillana\MIS\Desarrollos\Sysgold\
Procedimientos interinos del usuario	
Se han desarrollado Procedimientos interinos para los usuarios de la Aplicación? Si la respuesta es si, quien verificó que los Procedimientos de Recuperación en caso de Desastres de la Aplicación son todavía actuales y compatibles con los Procedimientos del usuario?	Si se han desarrollado. Existe un procedimiento para la toma manual de pedidos.
En donde se han almacenado los Procedimientos interinos de usuario? Quien tiene acceso al Procedimiento? (Se necesitan versiones electrónicas e impresas).	El procedimiento está en poder del Gerente de Ventas. Carlos Londoño tiene una copia impresa.
Cuando se verificaron los Procedimientos interinos de usuario o planean ser verificados?	Se han verificado cuando los vendedores por alguna razón tienen un problema con la máquina, mientras no tienen acceso al sistema por el inconveniente entonces se aplica el procedimiento interino.
Los clientes del negocio mantienen pistas diarias de la información entrada en la Aplicación? Serían ellos capaces de recuperar la información que se puede perder debido a un Desastres?	No en todos los casos.

Tabla 8.1: Test de Chequeo de Aplicaciones (Continuación)

Lista de Chequeo	Comentarios
Procedimiento de almacenaje	
En donde se han almacenado los Procedimientos de Recuperación de la Aplicación en caso de Desastres, a fin de que estén disponibles para el personal de los sistemas de negocio (Se necesitan versiones electrónicas e impresas).	Están disponibles en la Intranet de Perú, http://cosaaw01.kcc.com/Auditoria/PROCEDIMIENTOS/index.htm Procedimiento ITS – 023.
Conocen todos los miembros del team de ITS responsables de la aplicación como obtener una copia del procedimiento? Si no, cuando serán notificados?	El responsable es Carlos Londoño, quien conoce en donde obtener una copia. También el Jefe de ITS tiene copia impresa de todos los procedimientos.
Tienen los miembros del team de ITS responsables de la Aplicación otra documentación de soporte del sistema (electrónica e impresa) que esté disponible y actualizada? Si es así, donde se puede localizar y ser obtenida fácilmente? Cuando fue verificada o se planea verificar?	Carlos Londoño cuenta con la documentación del sistema. Se localiza en la ruta : COBTFN01/Santillana/MIS/Desarrollos/SYSGOLD
Verifique exactitud del Procedimiento	
Quién además del revisor revisó y verificó la exactitud de este Procedimiento de Recuperación de la Aplicación en caso de Desastres? En qué fecha fue verificada o se planea verificar?	El auditor de sistemas, Juan Daniel Giraldo verificó el procedimiento en Octubre 2007.
El team de ITS de la Aplicación está seguro de que los programas ó cronogramas de backup (archivos y datos) están en sincronía si una Recuperación fuera necesaria? Si los cronogramas de backup no pueden ser coordinados, está el team de ITS de la Aplicación conciente de las diferencias en el cronograma?	Carlos Londoño manifiesta estar seguro.
Está el team de ITS de la Aplicación conciente de las horas de ejecución del software de respaldo y ha verificado que este se complete antes de que sea recogido para el almacenaje off-site?	Carlos Londoño verifica los respaldos realizados periódicamente.
El team de ITS de la Aplicación ha revisado este Procedimiento y ha verificado que los pasos de Recuperación son todavía relevantes?	Si
Está el team de ITS de la Aplicación conciente de cualquier cinta o archivos que son críticos para la Recuperación de la aplicación y se han asegurado que estos estén documentados en este procedimiento.	Si

Tabla 8.1: Test de Chequeo de Aplicaciones (Continuación)

Lista de Chequeo	Comentarios
El team de ITS de la aplicación ha documentado si existe cualquier cinta(s) ó archivos dentro de la Recuperación de esta Aplicación que deba ser recuperada antes que otros?	No hay ninguna secuencia en particular.
Para aplicaciones basadas en servidor, el team de ITS de la Aplicación requiere cualquier componente específico de la Aplicación que deba ser instalado en el servidor? Se han hecho revisiones a los componentes específicos desde la última actualización del Procedimiento de Recuperación de la Aplicación en caso de Desastres, a fin de incluir los nuevos componentes?	Si. El SQL Server, IIS y servicios de FTP deben estar correctamente instalados y configurados.
Si la aplicación está basada en ambiente web y requiere seguridad en páginas web específicas, se han documentado esos requerimientos específicos en este Procedimiento de Recuperación de la Aplicación en caso de Desastres?	La aplicación no es ambiente WEB. El servidor tiene un grupo de control de usuarios, que tienen capacidad de FTP. Además los usuarios deben estar habilitados para hacer conexiones tipo RAS y contar con tarjetas SecurID.
Si la aplicación tiene grupos de seguridad asignados en el *Group Manager*, el team de ITS de la aplicación está seguro de que éstos son listados en este procedimiento?	Si está seguro.
Test reales del Procedimiento	
Se han probado los Procedimientos de Recuperación de la Aplicación en caso de Desastres durante una prueba real de recuperación de la plataforma? Si es así, en cual fecha fue probada y/o para cuando se ha programado la siguiente prueba?	La última prueba se realizó en Febrero 2008. .
Si fue así, quienes fueron los participantes (ITS/usuarios)?	Los participantes fueron Carlos Londoño, Juan B. Mesa, Andrés Felipe García y personal de Sysgold.
Se hicieron cambios a los Procedimientos de Recuperación de la Aplicación en caso de Desastres para resolver problemas que surgieron durante el ultimo test de Recuperación?	Si se creó un manual de la nueva instalación el cual se encuentra en: S:\Santillana\MIS\Desarrollos\Sysgold\Manuales\Sysgold - Guia de Instalacion mSales Web Server.doc
Para las aplicaciones críticas corriendo en mainframes, están los nombres de los data sets incluidos en la sección C.x.d del Procedimiento de Recuperación de la Aplicación? En que fecha se verificó o se planea verificar?	N/A

Tabla 8.1: Test de Chequeo de Aplicaciones (Continuación)

Lista de Chequeo	Comentarios
Para las aplicaciones críticas corriendo en mainframes, están los nombres de las bases de datos de acuerdo a lo documentado en la Sección C.x.c?	N/A
Para aplicaciones tipo *legacy* que corren en mainframes, están los data sets de los respaldos off-site identificados en el Procedimiento de Recuperación Sección D.2? ? En que fecha se verificó o se planea verificar?	N/A
La aplicación requiere respaldo de archivos por aspectos legales, contables o de impuestos? Si es así, están estos respaldos guardados off-site con el apropiado requerimiento de retención de registros de acuerdo al estándar corporativo?	No requiere.
Verificación final del Procedimiento	
En que año entró en producción esta aplicación? Se ha asegurado usted que todos los componentes de infraestructura, los requerimientos del volumen de datos, cronogramas de respaldos, grupos de seguridad, etc. que son utilizados por la Aplicación, han sido verificados y documentados dentro de este Procedimiento de Recuperación de la Aplicación en caso de Desastres, a fin de asegurarse de que todavía son precisos y exactos ?	Entró en producción Julio 1999.
Tiene usted confianza de que en el evento de un desastre, este procedimiento proveerá toda la información requerida para que la aplicación sea recuperada transparente y exitosamente? (Se recomienda que se piense sobre los pasos reales tomados para recuperar esta Aplicación).	Carlos Londoño, responsable de la aplicación, manifiesta que sí.

Fuente: Cía. Clark S.A.
Elaborado por: Johanna Sánchez, Luis Fierro

Modelo de Aprobación

Preparado Por:

Nombre	Firma	Título / Departamento	Fecha
		ITS	

Aprobado Por:

Nombre	Firma	Título / Departamento	Fecha
		ITS	

Autorizado Por:

Nombre	Firma	Título / Departamento	Fecha
		ITS	

8.3. MODELO DE ACTA DE PRUEBA DEL PLAN DE CONTINGENCIA

LOGISTICA-FACTURACIÓN – 2008

Con la premisa de que debemos estar preparados para cualquier tipo de eventualidades parciales o totales de nuestras instalaciones. El departamento de ITS se ha preparado para realizar la siguiente prueba del plan de contingencia.

El siguiente documento respalda las diferentes actividades realizadas durante el proceso.

1. INFRAESTRUCTURA DEL LOCAL.

Entre el 12 y 16 de noviembre de 2008 se ha procedido a dejar listo el sitio de contingencia dejando instaladas los paquetes y probando con éxito el enlace de Internet. Y el ingreso al sistema SAP y su correspondiente impresión.

2. PROCEDIMIENTOS Y FORMATOS UTILIZADOS

El procedimiento que se esta aplicando es el STM08, este procedimiento es para continuación de la operación. Los formatos utilizados serán documentos para facturas y guías de remisión.

3. ÁREAS INVOLUCRADAS.

Las áreas involucradas en el ejercicio del plan son:

ITS KCE	(Vicente Vanegas).	Créditos (Patricia Guzman).
Logística	(Nelson Alvarado).	Auditoria(Manuel Ruiz)

Las asignaciones por usuario las dará cada uno de los encargados de las áreas involucradas, los cargos que intervienen están el procedimiento de recuperación del negocio.

4. PRUEBAS DE CONTINGENCIA.

Para el día 17 de diciembre del 2008 se realizó la prueba de contingencia con el personal ya comunicado por mail. Esta prueba es una capacitación del plan, la prueba se baso en realizar un simulacro de contingencia, para lo cuál se movilizó al personal a la ciudad de Babahoyo donde quedan las instalaciones del centro de computo alterno, se tomaron los tiempos para medir el punto y tiempo de recuperación. Las pruebas son sustentadas con toda la información recolectada y los resultados que arrojaron los hechos.

5. DOCUMENTACIÓN

Una vez realizada la prueba se procedió a las respectivas correcciones del caso y actualizaciones del plan de contingencia en los diferentes sitios (Banco, Caja de seguridad y documentos internos).

CAPÍTULO IX

9. ANÁLISIS Y CONCLUSIONES

9.1. ANÁLISIS

En nuestra visita a las instalaciones del área de sistemas de la Compañía Clark S.A. observamos situaciones que fueron expuestas a análisis, para lo cuál podemos decir:

- Los resultados que arrojaron fueron favorables para la compañía, está a su vez debe analizar la implementación de un BCP que salvaguarden sus activos.
- No existieron dificultades para la realización del plan ya que la empresa nos dio todas las facilidades para cumplir con el trabajo.
- Los resultados a través de pruebas de control fueron los esperados, aunque está expenso a modificaciones cuando se amerite.
- Las actividades que no fueron visualizadas en el proceso son:
  1. Emergencias de edificios y procedimientos de evacuación.
  2. Recuperación de las diferentes unidades y departamentos de la Compañía.
  3. Equipos no relacionados con la red de datos (PBX, máquinas de fax, fotocopiadoras, etc.)

- Para la realización del plan contamos con la colaboración de todos los que conforman el departamento de sistemas y el área de administración de seguridad de la misma.
- El plan justifica su implementación mediante el análisis financiero y operacional, debido a que mayor es el beneficio que obtiene la empresa a los costos que se incurren al implementarlo.

9.2. CONCLUSIONES

Luego del análisis y desarrollo del Plan de Continuidad de Negocios del área de Sistemas para la empresa Clark S.A. podemos concluir lo siguiente:

- El plan es eficiente ya que cumple con todos los procedimientos específicos para su realización, el mismo está soportado en su análisis financiero y operacional.
- Este plan fue diseñado para una empresa industrial, se puede implementar para los demás sectores con ciertas estructuraciones, ya que la plataforma es la misma.
- La manufactura y el portafolio de productos que ofrece la compañía es pensando en la necesidad y satisfacción del cliente, cumpliendo así con todos los estándares de calidad para lo cuál el esfuerzo

diario que realiza con sus colaboradores hacen que las operaciones de la misma sean eficientes.

- La compañía tiene ciertos procesos establecidos que aseguran el bienestar de sus empleados, su infraestructura y equipos. Estos procesos son monitoreados por departamento de Administración de Seguridad de la compañía.
- La asignación de recursos se efectúa mediante una planificación financiera que es dirigida por la gerencia. Los recursos de la compañía son administrados eficientemente por cada departamento.
- La Cía. Clark S.A. cuenta con la infraestructura adecuada, la cumple con los estándares más altos de seguridad apropiados para sus operaciones diarias.
- La Cía. Clark S.A. cuenta con el personal adecuado y capacitado según la responsabilidad y actividad que realice. Además observamos que para el departamento de Sistemas el perfil de cada colaborador es el adecuado para ocupar el cargo correspondiente.
- La Cía. Clark S.A. tiene los sistemas de información necesarios para su funcionamiento, además cuenta con el soporte que proporcionan sus proveedores que le brindan un servicio de calidad.

- La Cía. Clark S.A. cuenta con buenas expectativas a futuro ya que cuenta con el respaldo de sus componentes principales que le agregan valor: los clientes que están satisfechos con el producto, los colaboradores que están cómodos con el ambiente de trabajo y los beneficios de la compañía, y la eficiente administración de sus recursos hace que vean el crecimiento admirable de la misma, siempre innovando con nuevas oportunidades para presentarlas al mercado y ante todo ayudando al medio ambiente. Esto hace que la compañía tenga permanencia y sea sostenible en el tiempo.

- Finalmente agregamos que la mayor parte de los problemas que se sucitan en la compañía son operativos, pero estos a su vez son suplidos por manuales departamentales para el debido caso. Citamos algunos ejemplos de los problemas que se presentan:

Área de Producción:

- ✓ Daño de maquinaria, Instalación y mantenimiento de la misma

Área de Logística y Distribución:

- ✓ Guías de remisión

Área de IT:

- ✓ Desconfiguración de equipos, instalación de programas.
- ✓ Sobrecarga de Transacciones.

ANEXOS

ANEXO 1: Serias Exposiciones al riesgo

La siguiente tabla identifica las exposiciones mas serias de la localidad que se encuentra la compañía. La información fue basada en registros obtenidos del K-C Propery Insurance Carrier (FM Global). Las localidades listadas en la tabla deberían usar esta información para ayudarse a identificar y clasificar la vulnerabilidad a estas amenazas, y así determinar una localidad apropiada para almacenar los respaldos de información.

Localidad	Exposición a inundaciones		Terremoto	Altos
	100 años	500 años	Zona 40	VIENTOS
Argentina (ambas localidades)			X	
Australia, Warwick Farm	X	X		
Bolivia (todas las localidades)			X	
Bolivia, Santa Cruz	X	X		
Brasil, El dorado	X	X		
Chile (todas las localidades)			X	
Colombia, Cali			X	
Colombia, Pereira			X	
Costa Rica (todas las localidades)			X	
Costa Rica, Cartago	X	X	X	
Ecuador (todas las localidades)			**X**	
El Salvador			X	
France, Rouen	X	X		
Germany, Mainz	X	X		
Guatemala			X	
Honduras			X	
Indonesia			X	
Italy, Patrica	X	X		
Italy, Romagnano	X	X		
Italy, Villanovetta	X	X		
Korea, Taejon	X	X		
Mexico (todas las localidades, excepto) Ramos)			X	
Peru (todas las localidades)			X	
Philippines (todas las localidades)			X	
Switzerland, Balsthal	X	X		
Taiwan, Tayuan	X	X		
Thailand, Panthumthani		X		
Thailand, Samut Prakern	X	X		
Thailand, Songkhla (SafeSkin)	X	X		
USA, Chester PA (Mill)	X	X		
USA, East Ryegate VT		X		
USA, Fullerton, CA		X	X	
USA, Haltom City TX (Technol)	X	X		
USA, Jenks				X
USA, Mobile				X
USA, Neenah WI (Neenah Paper)	X	X		
USA, New Milford CT	X	X		
USA, Owensboro KY	X	X		
USA, Paris, TX				X
USA, San Diego (SafeSkin)			X	

ANEXO 2: Lista de chequeo de las instalaciones Computacionales

La siguiente tabla contiene una lista de chequeo general de preguntas, para ayudar en la determinación de las vulnerabilidades potenciales de las instalaciones computacionales. Responda cada pregunta y provea comentarios tanto como sean necesarios. Basada en las instalaciones de procesamiento, no todas las preguntas serían relativas a todas las instalaciones. Indique No Aplicable (N/A) para aquellas preguntas que no serían aplicables a esas instalaciones.

Lista de chequeo de las Instalaciones Computacionales	Si	No	Comentarios
Access Controls			
¿Está el acceso a la sala de computadoras restringida a personal seleccionado? Si es así cómo.	X		Existe un sistema de control de acceso a la sala de servidores y telecomunicaciones, el cual se basa en un software, tarjetas magnéticas, puntos de acceso a puertas (candados) y un equipo de control principal.
¿Está la lista de accesos actualizada, y que tan a menudo se hace?	X		Los accesos se registran automáticamente en el software de control, cada vez que el personal autorizado utiliza su tarjeta magnética para abrir la puerta de la sala.
¿Dónde se localiza la lista de acceso? Cómo es controlada?	X		Las listas de accesos residen en una base de datos, el cual corre en una PC físicamente instalada en la sala de la PBX. Sólo el LAN Administrator y el ITS Manager tienen acceso a esta sala y ambos tienen acceso al software.
¿Son utilizados llaves, candados o algún otro dispositivo para controlar el acceso?	X		Se utilizan las tarjetas magnéticas.
¿Como se controlan las llaves?			Las tarjetas son provistas por el Coordinador Administrativo. Luego estas se codifican en el software, para habilitarlas el acceso a la sala de servidores y telecomunicaciones.
¿Se han establecido procedimientos para visitantes? Si es así, son estos efectivos?	X		Para permitir el acceso a las instalaciones de las oficinas, el LAN Adm. o el MIS Manager debe solicitar el permiso al encargado de seguridad del edificio, indicando objetivo, fecha de entrada y salida y compañía a la que representa. Todo visitante es acompañado por el LAN Admin el ITS Manager mientras está en la sala. Existe una bitácora de entrada de visitantes a la sala de servidores y telecomunicaciones.
¿Si se utilizan tarjetas de acceso, están éstas inventariadas y controladas?	X		Si se lleva control

Lista de chequeo de las Instalaciones Computacionales	Si	No	Comentarios
Access Controls			
¿Existe energía de reserva para operar las puertas controladas electrónicamente, durante un fallo de energía? Si no es así, cómo se controlan las puertas durante una falla de corriente?		X	Si la energía falla el mecanismo electrónico de control de acceso, existe un candado convencional que se abre desde afuera. La llave de este candado está custodiada por el MIS Manager.
¿Cómo se controla el acceso a la sala de computadores para el personal de custodia, eléctrico y de mantenimiento?			El personal de mantenimiento es acompañado por el LAN Admin el ITS Manager mientras está realizando su trabajo, su fecha y hora de entrada y salida es anotada en la bitácora existente en la sala para el control de acceso.
Limpieza			
¿Son la sala de computadores, el piso y oficinas limpiadas y aspiradas regularmente?	X		Actualmente el personal de limpieza hace el aseo cada 2 semanas. Se hace registro en la bitácora de control de acceso.
¿Está prohibido comer y fumar dentro de la sala de computadores?	X		
¿Existe un área separada para el descanso del personal de operaciones?	X		Todo personal de ITS, al igual que el resto de empleados de utiliza una cafetería localizada dentro de las oficinas.
¿Son las cubiertas del equipo y servicios limpiados regularmente?	X		La labor de limpieza se realice cada 2 semanas.
FUEGO			
¿Son los operadores entrenados periódicamente en técnicas de combate contra el fuego, y tienen responsabilidades asignadas individualmente?	X		Se realiza un entrenamiento anual en el cual participan todos los empleados de la compañía, incluyendo el personal de ITS.
¿Los individuos asignados están familiarizados con sus responsabilidades en emergencias?	X		El personal de ITS está entrenado para responder en caso de emergencias.
¿Están el papel y otros suministros, excepto aquellos requeridos para operar, almacenados fuera del área de computadores?	X		Existe una pequeña bodega en donde se guardan tarjetas, y switches de repuesto.
¿Están las salidas de incendios marcadas claramente?	X		
¿Están los Planes de Emergencia en caso de Incendio claramente publicados?	X		El Edificio es propiedad de la compañía, se rige por las normas de seguridad.
¿Existen extinguidotes portátiles localizados estratégicamente alrededor del área, con indicaciones claramente visibles?	X		Existe un extintor de incendio localizado dentro de la sala de servidores y telecomunicaciones, y otro localizado afuera de la sala, contiguo a la puerta de entrada.
¿Ha sido el personal de operaciones claramente instruido en las acciones requeridas en el evento de una emergencia?	X		El personal de ITS recibe una capacitación anual para reaccionar en el caso de un desastre.

Lista de chequeo de las Instalaciones Computacionales	Si	No	Comentarios
FUEGO			
¿El sistema de detectores de humo/fuego es probado regularmente	X		Fecha de ultima verificación – Junio 05- -2004
¿Se conducen ejercicios de incendio regularmente Cuándo se condujo el ejercicio por última vez?	X		Junio-11-2004 se realizo un simulacro de evacuación en el edificio.
¿Existen luces de emergencia de baterías a través de la sala de computadores? Si así, son operacionales?	X		Ubicadas en todos los centros de cableado
¿Las salidas están marcadas claramente	X		
¿Las luces de salida son operacionales?	X		Cada centro de comunicaciones tiene las respectivas luces de salida.
¿La cuadrilla de emergencia tendría acceso a la sala e computadores sin retardo?	X		El LAN Adm. y ITS Manager son parte de la cuadrilla de emergencia. Pero nadie más de la cuadrilla de seguridad podría tener acceso en emergencia.
Hardware			
¿Son las actividades de mantenimiento programadas y monitoreadas para asegurar rendimiento y confiabilidad apropiados?	X		
¿Es el mantenimiento realizado sobre una base de programación regular?	X		
Procedimientos de Operación			Las Oficinas de ITS no tienen personal dedicado a realizar funciones e operación.
¿Están los procedimientos de operación vigentes?			N/A
¿El sistema de distribución previene que personas autorizadas reciban reporte con información sensitiva y/o clasificada? Los procedimientos son adecuados?			N/A
Existen procedimientos para procesar, marcar y manejar material clasificado?			N/A
¿El personal de operaciones está familiarizado con los procedimientos?			N/A
¿Como son reportadas las violaciones?			N/A
¿Existen procedimientos para el *shut down* de los sistemas operativo?	X		Si existe y se encuentra impreso en la sala de Servidores
¿Se han establecido procedimientos que provean una guía sobre los pasos a seguir en el evento de una falla de los equipos?	X		Procedimiento ITS-004
¿Está el personal de operaciones familiarizado con los términos de los contratos de mantenimiento, en relación con los períodos principales y los períodos por llamada?	N/A		
¿Está el personal de operaciones completamente instruido sobre las técnicas para mantener un ambiente apropiado en la sala de computadores?	N/A N/A		

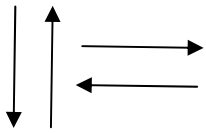
Lista de chequeo de las Instalaciones Computacionales	Si	No	Comentarios
Suministros			Los suministros son controlados por el Administrador de las oficinas, no por ITS.
¿Existe un sistema que asegure que un adecuado pero no excesiva provisión de suministros está disponible (cintas magnéticas, cartuchos de impresoras, papel tabulado y formas especiales)?			N/A
¿Existen áreas de almacenamiento adecuados y éstas cumplen los estándares ambientales requeridos para el almacenamiento de suministros?			N/A
Training			
Is there an effective cross training program?		X	
Are individual training records up-to-date?		X	
Has a training coordinator been appointed?		X	
Are manufacturers operating manuals kept in the computer room? If so. Are they current?	X		AS400
Are operator run books kept in an up-to-date condition in the computer room?			N/A

ANEXO 3: Simbología del Diagrama Paso a Paso de Recuperación

Principio/ Fin, parada de proceso.

Proceso en general. Operaciones definidas que originan cambios.

Modificación de programa; instrucción que modifica a otra, o inicialización de rutinas.



Secuencia y dirección del flujo

BIBLIOGRAFÍA

1. AKHTAR SYED PH.D, AFSAR SYED BMATH **"Business *Continuity Planning"***, 2004.

2. STANLEY B. BLOCK, GEOFFREY A. HIRT ***"Fundamentos de Gerencia Financiera"***, MC GRAW-HILL. NOVENA EDICIÓN, 2002.