CAPÍTULO I

INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

A finales del siglo 20, los sistemas informáticos se constituyeron en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial.

Hoy la informática, está enrolada en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar sometidas a las leyes generales de la misma. En consecuencia, las organizaciones informáticas forman parte del denominado “gestión de la empresa”. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existen los Planes de Contingencia.

En la última década los cambios informáticos en el Ecuador fueron de mucha importancia, la adquisición de tecnologías tanto en el área de software y hardware

permitieron a las empresas públicas y privadas desarrollar nuevos sistemas informáticos que se ajustan a sus necesidades, y también el área de hardware actualizando sus sistemas de comunicación, vigilancia, control de personal, redes de computadores, comunicaciones IP, etc. Del mismo modo que las tecnologías de software y hardware se desarrollan, también surgen problemas, la empresa pública y privada aun no toma conciencia sobre los resultados catastróficos que tendrían si algún tipo de problema surgiera en sus servidores informáticos o en cualquiera de sus sistemas de comunicación.

Así tenemos que la gran cantidad de computadores, sistemas automatizados y de comunicación se encuentran desprotegidos por problemas y falta de planificación, percances eléctricos, naturales, sabotajes o daños excepcionales sin predicción, la piratería de software, como también el personal calificado hace que se hayan creado procedimientos para este tipo de anomalías.

1.2 ANTECEDENTES

Actualmente, Quito posee un parque industrial distribuido por toda la provincia, la creciente demanda de espacios para complejos industriales ha permitido que estos se desarrollen por toda la provincia sin que estos se encuentren centralizados y al contrario estos son implementados bajo controles municipales de construcción, Cuerpo de Bomberos, Cruz Roja, pero poco o nada se ha desarrollado sobre el campo informático, es así que, en poco porcentaje de estos conjuntos industriales tienen reglamentos para el desarrollo del área informática en sus empresas, y en menos porcentaje un plan de contingencia informático que permita actuar en caso de emergencias.

La falta de reglas, reglamentos y documentos hacen que la mayoría de empresas que componen un conjunto industrial desarrollen procesos empíricos para poder salvaguardar sus componentes informáticos de manera independiente, produciendo de esta manera la repetición de procesos, subutilización y sobre carga de controles dentro del conjunto industrial.

El Conjunto de Bodegas PARKENOR ha tenido un proceso evolutivo vertiginoso, y el área informática no ha sido la excepción, en los últimos cinco años su desarrollo informático fue rápido, sus procesos manuales fueron reemplazados por procesos automatizados tales como contabilidad, control de personal, control de la seguridad, video vigilancia, correo electrónico, etc. Adicionalmente las empresas que constituyen el Conjunto de Bodegas PARKENOR desarrollaron paralelamente sus necesidades informáticas de tal manera que se crearon la misma cantidad de necesidades que empresas tiene el Parque Industrial.

El Sistema Informático combina procesos manuales y automatizados en de área de cobros, información, control de voltaje, alimentación, control de transporte, inventarios los cuales al tener algún tipo de improviso llevarían a el conjunto de empresas a tener fuertes pérdidas económicas.

Todo este crecimiento acelerado que desarrolló el Conjunto Industrial creó una nueva necesidad y es proteger el sistema informático en caso de desastres ya sean estos naturales, incendios, intencionales, eléctricos, comunicaciones, y todo tipo de percances que se produjeren y que atente contra el desarrollo normal del sistema informático del Conjunto de Bodegas PARKENOR.

1.3 SITUACIÓN ACTUAL

El Conjunto de Bodegas PARKENOR no tiene un Plan de Contingencia Informático, por tal razón el Conjunto Industrial posee reglas básicas para una necesidad general, podemos decir que PARKENOR adolece de los siguientes estudios:

- Análisis de Riesgos de Sistemas Críticos que determine la tolerancia de los sistemas.
- Establecer una etapa crítica de recuperación, donde los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas y establecer las prioridades del proceso.
- Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.
- Designar un Centro Alternativo de Proceso de Datos.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores de respaldos (Back-up).

Además el área de construcción que garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de datos, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que se puedan derivar.

Un concepto aplicable a cualquier actividad, no sólo en informática, donde las personas hagan uso particular o profesional de entornos físicos, en caso del Conjunto de Bodegas PARKENOR por su desarrollo vertiginoso no pudo ser tomado en cuenta, Así tenemos:

- Ubicación del edificio.
- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

Además en el desarrollo del proyecto no fueron tomados en cuenta seguros para afrontar Pérdidas de Procesos Informáticos del siguiente tipo:

- **Centros de proceso y equipamiento:** Cobertura sobre el daño físico en el CPD (Centro de Procesamiento de Datos) y el equipo.
- **Reconstrucción de medios de software:** Cubre el daño producido sobre software tanto los que son de propiedad de la empresa como aquellos que constituyen su responsabilidad.

- **Gastos extra:** Cubre gastos que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos. Es suficiente para compensar los costos de ejecución del plan de contingencia.
- **Interrupción del negocio:** Cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.
- **Documentos y registros valiosos:** Se contrata para obtener una compensación en el valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de reconstrucción del software.
- **Errores y omisiones:** Proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.
- **Cobertura de fidelidad:** Cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.
- **Transporte de medios:** Proporciona cobertura ante pérdidas o daños a los medios transportados.
- **Contratos con proveedores y de mantenimiento:** Proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

1.4 JUSTIFICACIÓN

El Conjunto de Bodegas PARKENOR, es un conjunto industrial que se encuentra al norte de quito en la avenida 10 de Agosto km 5.5, durante los últimos cinco años PARKENOR se desarrolló de manera acelerada en el área tecnológica, la necesidad de actualizar sus computadores, impresoras, internet, seguridad digital, enlaces de red, correo electrónico fueron una necesidad imperiosa para su éxito en los negocios, este desarrollo tecnológico apresurado creó un nuevo problema que se resume en el cuidado, previsión de daños del área informática, es decir PARKENOR necesita realizar un conjunto de procedimientos y reglas a seguir en caso de accidentes que afecten de alguna manera los sistemas informáticos del Conjunto Industrial.

Es así, que la falta de dichos reglamentos y reglas por más de una vez han sido los causantes de pérdidas económicas, pues al no tener un Plan de Contingencia Informático el personal no ha sido capaz de actuar eficientemente en casos de inundaciones, fallas eléctricas, robos de computadores, virus, incendios, seguridad y peor aun si cualquier accidente humano o industrial sucediese en horas no laborables.

El Conjunto de Bodegas PARKENOR al estar constituido por varias empresas, sus asociados han visto en la necesidad de crear acciones empíricas en caso de accidentes en los sistemas de información, de esta manera contribuyen inconscientemente para que los procesos por lo menos se dupliquen y del mismo modo el esfuerzo humano sea vano, asociándose a la desesperación de no contar con un Plan de Contingencia Específico para el conjunto en pleno.

1.5 LISTA DE ALMACENES DEL CONJUNTO PARKENOR

El Conjunto de Bodegas PARKENOR está constituido por 65 bodegas 10 almacenes y 1 patio de comidas de los cuales la mayoría están establecidas definitivamente y otras que permanecen alquiladas o en comodato, ponemos a disposición el listado de bodegas y almacenes que a esta fecha se encuentran funcionando en el parque industrial.

Tabla No. 1.1 Almacenes que conforman el Conjunto de Bodegas PARKENOR

BCO. GUAYAQUIL	**DISTRITEX**	**GARMENT**
XAFEL	**PINTURI**	**IMPORDEMIN**
R. FERRY	**CYEDE**	**GERCASA**
JUVENTUS S.A.	**IMPORDEMIN**	**TEXPRINT**
PROTECOMPU	**DISBERRNER**	**MARUYAMA**
DISTRITEX	**REAL TEXTIL**	**STAUTON**
SINDIMED	**SUPER EXTRA**	**MECADEC**
EUROCOSMETICA	**GUIBOGA**	**SONAR LTDA.**
PERFUMESSA	**SAJADOR**	**VALERO S.A.**
DATALOG	**DISTRILINK**	**JOLASUR S.A.**
COLPIZAMOTOR	**ABRACOL**	**FORROTEXAS**
DIBEAL S.A.	**FCL IMPORT**	**REJAPONSA**
GLOBAL FLUIDS	**CELLSYSTEM**	**FUND. ECUADOR**
ECUACOLOR	**SOLO ECUADOR**	**INDUTEXMA**
ETIQUETASA	**ANTURIOS CIA.**	**AGROINDUSTRIAL**
OFICCE ECUADOR	**CORPSTARS**	**TROFEOS CASTRO**
TRENSAD ECUADOR	**GAMAPARTES**	**TEXAECUADOR**
YAKUTHANY	**VALERO S.A.**	**MUNI HOME**
DISMODAS	**SIGLO 21**	**SOCK SHOP**
PONDARMAT	**PANBOEC**	**SINE**
DIST. DESCALZI	**BAKERY CIA.**	

El Administrador del Conjunto Industrial ha tomado la iniciativa de realizar el Plan de Contingencia, para que un futuro cercano dicha necesidad sea cubierta y de esta manera seguir a la par de la tecnología.

1.6 OBJETIVOS

1.6.1 Objetivo General

Desarrollar el Plan de Contingencia Informático del "CONUNTO DE BODEGAS PARKENOR".

1.6.2 Objetivos Específicos.

1. Desarrollar el Marco Teórico del proyecto.
2. Identificar los riesgos y soluciones del siniestro
3. Usar un lenguaje común con el personal de la Institución
4. Definir roles y las acciones del personal de PARKENOR.
5. Desarrollar un Plan de Continuidad de Negocios.
6. Capacitar al personal de la PARKENOR
7. Desarrollar un Plan de Recuperación de Desastres..
8. Velar la integridad del personal de PARKENOR.

1.7 ALCANCE

El presente proyecto de tesis tiene previsto realizar el estudio e implementación del Plan de Contingencia para APRKENOR que incluye los alcances a las siguientes áreas:

1.7.1 Área Física.

Tiene como tarea específica analizar el diseño y construcción del edificio donde están ubicados los sistemas informáticos del Conjunto de Bodegas PARKENOR, así tenemos:

- Sección eléctrica
- Sección hídrica

- Tipo de construcción
- Ubicación de la construcción
- Acceso al edificio.
- Seguridad.
- Control de incendios.
- Áreas de almacenamiento informático.

1.7.2 Área Software.

Tiene como tarea específica analizar y estudiar el Software y los Sistemas de Información que se desarrollan en el Conjunto Industrial, así podemos tener:

- Software legal
- Software ilegal (Pirata)
- Virus
- Acceso de personal no autorizado
- Respaldos
- Impresiones
- Programas especializados
- Control de internet
- Redes, accesos remotos, comunicación de datos.
- Perdida de información.

1.7.3 Área Hardware.

Tiene como tarea específica analizar el buen funcionamiento electrónico de los equipos informáticos, periféricos, comunicación, y seguridad estos pueden ser:

- Impresoras
- Monitores
- Fuentes de poder
- CPUs
- Faxes
- Estructuras de red, Cables, Switchs, Tarjetas de red.
- UPS.
- Unidades externas de almacenamiento. Ejemplo DVD, CD.
- Cámaras.
- Cableado de datos.

1.7.4 Área de Personal.

Este proceso permitirá establecer el nivel de instrucción que posee el personal a cargo, de esta manera se podrá desarrollar informes de responsabilidad y tolerancia en sucesos posteriores, así podemos definir:

- Grado de responsabilidad
- Grado de adiestramiento de personal
- Ingreso de personal no autorizado
- Pérdida de información
- Reportes

CAPÍTULO II

MARCO TEORICO

2.1 ¿QUÉ SON LOS SISTEMAS DE INFORMACIÓN?

Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como cuando una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo la mayor parte de los sistemas son más complejos que el enunciando anteriormente. Normalmente una organización tiene más de un sistema de computadoras para soportar las diferentes funciones de la organización, ya sean de ventas, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que permitan continuidad en la operatividad de los sistemas para no ver afectados los

objetivos de las mismas y no perder la inversión de costos y tiempo.

2.2 ¿QUÉ ES UN PLAN DE CONTINGENCIA?

Podríamos definirlo como una estrategia planificada con una serie de procedimientos que faciliten u orienten a tener soluciones o alternativas que permitan restituir rápidamente los servicios de la organización ante una eventualidad que pueda paralizar la empresa, ya sea de forma parcial o total.

El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de una empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

2.3 TIPOS DE CONTINGENCIAS

En el Plan de Contingencia Informático se establecen procedimientos preventivos para el manejo de casos de emergencia que se presenten en el Conjunto de Bodegas PARKENOR al sufrir una situación anormal, protegiendo al personal, las instalaciones, la información y el equipo.

En el momento que sea necesario aplicar el Plan de Contingencia, la reanudación de las actividades puede ser el mayor reto que enfrente el departamento de sistemas, probablemente no pueda regresar a su lugar habitual de trabajo o no disponga de las herramientas usuales para desempeñar normalmente sus actividades. Incluso es posible tener que desarrollar el trabajo sin el equipo de gestión y sus colaboradores.

No puede dejar el Plan de Contingencia para una ocasión posterior debido a cargas excesivas de trabajo, es necesario presupuestar tiempo y recursos para crear un programa de contingencia completo y útil.

La preparación ante un desastre comienza asegurándose de poseer los datos a recuperar. Un programa de contingencia no incluye solamente operaciones de copia de seguridad como parte de su contenido; sin embargo, la realización de copias de seguridad fiables es un requisito previo.

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Menor.- Es la que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.

Grave.- Es la que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de 24 horas.

Crítica.- Afecta la operación y a las instalaciones, este no es recuperable en corto tiempo y puede suceder por que no existen normas preventivas o bien porque estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural como un terremoto.

Tipos de Contingencias de acuerdo al grado de afectación:

- En el mobiliario.
- En el equipo de cómputo en general (procesadores, unidades de disco, impresoras etc.).
- En comunicaciones (hubs, ruteadores, nodos, líneas telefónicas).
- Información.
- Instalaciones.

2.4 OBJETIVOS DEL PLAN DE CONTINGENCIA

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

2.5 PLAN DE ACCIÓN GENERAL

- Realizar un levantamiento de los servicios informáticos.
- Llevar a cabo un Inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, Internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.
- Identificar un conjunto de amenazas.
- Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc.
- Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.
- identificar soluciones e identificar posibles soluciones erróneas
- Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.
- Se debe estar preparado para cualquier percance, verificando que dentro de la Dirección de Gobierno Digital se cuente con los elementos necesarios para salvaguardar sus activos.
- Crear la documentación pertinente que se utilizará en caso de activarse alguna contingencia.

- Implementar las contingencias.
- Monitorear y revisar documentación de acuerdo a necesidades posteriores.

2.6 PLAN DE RECUPERACIÓN DE DESASTRES

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

2.7 PLAN DE EMERGENCIAS

En este plan se establecen las acciones que se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

CAPÍTULO III

FASES PARA EL DESARROLLO DEL PLAN DE CONTINGENCIA PARA PARKENOR

Es importante tener presente que un plan de contingencia, mucho depende de la infraestructura de la empresa y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta es dar los puntos más importantes a tener en cuenta.

La presente metodología se podría resumir en ocho fases de la siguiente manera:

- **Planificación:** Preparación y aprobación de esfuerzos y costos.
- **Identificación de amenazas y riesgos:** Plan de seguridad física y lógica.
- **Identificación de soluciones:** Evaluación de Riesgos de fallas.
- **Estrategias:** Soluciones alternativas, procedimientos manuales.
- **Documentación del proceso:** Creación de un manual del proceso.
- **Realización de pruebas:** Soluciones que probablemente funcionen.
- **Implementación:** creación de soluciones, documentación de los casos.

- **Monitoreo:** Probar nuevas soluciones o validar los casos.

3.1 FASE 1: PLANIFICACIÓN

3.1.1 Diagnóstico

El Conjunto de Bodegas PARKENOR es una asociación de industrias donde su desarrollo rápido no les permitió crear un plan de contingencia informático, el que es necesario lo más pronto posible.

La falta de previsión de desastres en las áreas naturales, eléctricas, datos, accidentales o vandalismo hace urgente la implementación de un plan de contingencia.

3.1.2 Organización Estructural y Funcional.

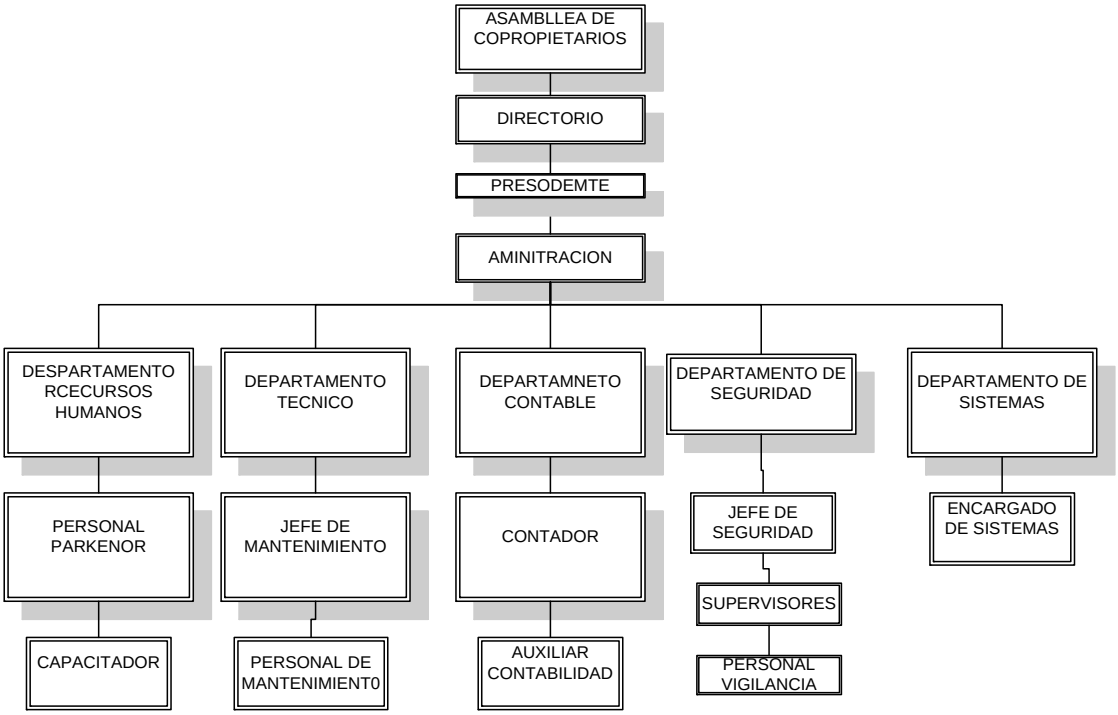

Figura 3.1: Organización Administrativa PARKENOR.

3.1.3 Lista de almacenes del conjunto PARKENOR

Tabla 3.1: Lista de almacenes PARKENOR.

1. BCO. GUAYAQUIL	2. DISTRITEX	3. GARMENT
4. XAFEL	5. PINTAURI	6. IMPORDEMIN
7. R. FERRY	8. CYEDE	9. GERCASA
10. JUVENTUS S.A.	11. IMPORDEMIN	12. TEXPRINT
13. PROTECOMPU	14. DISBERRNER	15. MARUYAMA
16. DISTRITEX	17. REAL TEXTIL	18. STAUTON
19. SINDIMED	20. SUPER EXTRA	21. MECADEC
22. EUROCOSMETIC	23. GUIBOGA	24. SONAR LTDA.
25. PERFUMESSA	26. SAJADOR	27. VALERO S.A.
28. DATALOG	29. DISTRILINK	30. JOLASUR S.A.
31. COLPIZAMOTOR	32. ABRACOL	33. FORROTEXAS
34. DIBEAL S.A.	35. FCL IMPORT	36. REJAPONSA
37. GLOBAL FLUIDS	38. CELLSYSTEM	39. DIST. DESCALZI
40. ECUACOLOR	41. SOLO ECUADOR	42. INDUTEXMA
43. ETIQUETASA	44. ANTURIOS CIA.	45. AGROINDUSTRIAL
46. GAMAPARTES	47. OFICCE ECUADOR	48. FUND. ECUADOR
49. SINE	50. TROFEOS CASTRO	51. TEXAECUADOR
52. YAKUTHANY	53. VALERO S.A.	54. MUNDI HOME
55. DISMODAS	56. SIGLO 21	57. SOCK SHOP
58. PONDARMAT	59. PANBOEC	60. TRENSAD
61. CORPSTARS	62. BAKERY CIA.	63. MAGIC CHIEF

3.1.4 Servicios y/o Bienes Producidos.

El Conjunto de Bodegas PARKENOR al ser un conjunto industrial desarrolla bienes y servicios los cuales detallamos de forma general.

- Servicios bancarios
- Servicios de seguridad
- Venta de electrodomésticos
- Venta de artículos textiles
- Venta de artículos inflamables
- Compara venta de chatarra
- Venta de artículos informáticos
- Venta de artículos de madera
- Venta de artículos de caucho y neumáticos
- Venta de pinturas y diluyentes
- Servicios alimenticios
- Venta de servicios de comunicación
- Almacenamiento de artículos varios
- Venta de textiles.
- Servicio de gasfitería, albañilería y electricidad
- Venta de electrodomésticos y línea blanca.
- Servicios de comunicaciones digitales.
- Venta de servicios y herramientas hidráulicas.
- Alquiler de bodegas y almacenes

3.1.5 Servicios y Materiales Utilizados.

PARKENOR por ser un conjunto industrial de acelerado crecimiento utiliza gran cantidad de servicios y materiales que son importantes para su desarrollo.

Tabla 3.2: Servicios y materiales utilizados por el Conjunto de Bodegas PARKENOR

EMPRESA	SERVICIO	TELEFONO
AGUA POTABLE QUITO	Agua	2501225
EMPRESA ELÉCTRICA QUITO	Electricidad	136
C.N.T	Telefonía convencional	1800222847
BOMBEROS	Emergencias	102
CRUZ ROJA	Emergencias, ambulancia	131
POLICIA	Seguridad policial	101
PARKENOR	Chatarra	02 2484004
PORTA	Telefonía CELULAR	*611
MOVISTAR	Telefonía CELULAR	1800 001 001
ANDINANET	Internet	1800 378 466
SEGUROS EQUINOCCIAL	Seguros privados	2 445602
TRANPORTE PERSONAL	Taxis	
TRANSPORTE DE CARGA	Carga	2420740
COOPERATIVA TARQUI	Transporte Liviano	2226516
GASOLINERA PETROECUADOR	Gasolina, diesel	
SEGURIDAD	Grupo LAAR	3960000
MAGIC CHEF	Alimentación	2801126

SEGURIDAD SOCIAL	IEES	www.iees.gov.ec
DEFENSA CIVIL	Emergencias	2469009
METRO DESING	Imprentas	2566331
SHARP	Copiadoras	2541600
MULTICOM	Comunicación	2432915
OFFICE AMERICA	Suministros de Oficina	2805732
PC PLUS	Informática	096851840
DHL	Transporte de paquetes	023975000
BANCO DE GUAYAQUIL	Bancos	2382010
PC PLUS	Informática	093166584
SERVIENTREGA	Correos	

3.1.6 Inventario de Recursos Informáticos.

El Conjunto de Bodegas PARKENOR al ser un conjunto industrial que está constituido por varias empresas, estas poseen áreas informáticas independientes, que utilizan los mismos proveedores en todo el conjunto industrial, todas las empresas poseen computadores, líneas telefónicas, internet, impresoras, módems, sistemas operativos Windows, editor de texto, hojas electrónicas, antivirus free.

Así podemos clasificar e inventariar el sector informático de cada una de las empresas. Ver tabla 3.3

Tabla 3.3: Inventarios utilizados por el Conjunto de Bodegas PARKENOR

EMPRESA	C.P.U.	IMP.	PROGRAMAS	OTROS EQUIPOS
ADMINISTRACIÓN	5	3	WINDOWS XP	ANTENA DE INTERNET
PARKENOR			MS OFFICE	2 LINEAS TELEFÓNICAS
			SISTEMA CONTABLE	1 ROUTER
			DVR SISTEMA DE	1 SWITCH
			VIGILANCIA	1 COPIADORA
			DVR REMOTO	1 FAX
				1 UNIDAD DE VIGILANCIA
				1 SCANNER
DISTRITEX	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	2 UPS
			SISTEMA DE INVENTARIOS	1 ROUTER
				1 SWITCH
				1 FAX
GARMENT	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	2 UPS
			SISTEMA DE INVENTARIOS	1 ROUTER
				1 SWITCH
				1 FAX
				1 CANER
XAFEL	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	
			SISTEMA CONTABLE	
PINTAURI	3	3	WINDOWS XP	1 LINEA TELEFÓNICA

			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
INPORDEMIN	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
JUVENTUS S.A	2	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	
			SISTEMA CONTABLE	
TEXPRINT	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	2 UPS
PROTECOMPU	3	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	2 UPS
				1 SCANNER
				1 FAX
DISBERNER	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	2 UPS
				1 FAX
MARUYA	4	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER

			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	3 UPS
				1 FAX
REAL TEXTIL	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
STAUTON	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 UPS
SINDIMED	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
				1 SCANNER
SUPER EXTRA	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	
MECADEC	3	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	
EURO	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
COMSMETICA			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX

				1 SCANNER
GUIBOGA	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
SONAR LTDA			WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	
PREFUMESA	3	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
SAJADOR	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
VALERO S.A	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
DATALOG	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
DITRILINK	4	4	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH

			SISTEMA CONTABLE	1 FAX
				1 COPIADORA
JOLASUR S.A	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
COLPIZA MOTOR	4	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
ABRACOL	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
FORROTEXAS	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	
			SISTEMA CONTABLE	
FCL IMPORT	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
REJAPONSA	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
GLOBAL FLUIDS	3	3	WINDOWS XP	1 LINEA TELEFÓNICA

			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
CELLSYSTEM	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
				1 COPIADORA
DIST. DESCALZI	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
ECUACOLOR	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
				SCANNER
SOLO ECUADOR	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
INDUTEXMA	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
ETIQUETASA	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	

			SISTEMA CONTABLE	
ANTURIOS CIA.	2		WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
AGROINDUSTRIAL	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
				1 COPIADORA
GAMAPARTES	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	1 SCANNER
			SISTEMA CONTABLE	
OFFICE ECUADOR	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
FUND. ECUADOR	4	4	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 UPS
				1 COPIADORA
SINE	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	1
			SISTEMA CONTABLE	
TORFEOS CASTRO	2	1	WINDOWS XP	1 LINEA TELEFÓNICA

			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
TEXA ECUADOR	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
YAKUTHANY	3	3	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
VALERO S.A	1	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1FAX
			SISTEMA DE INVENTARIOS	1 UPS
			SISTEMA CONTABLE	1 SCANNER
MUNDI HOME	1	1	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 FAX
			SISTEMA DE INVENTARIOS	1 COPIADORA
			SISTEMA CONTABLE	
DISMODAS	4	4	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
SIGLO 21	6	6	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	3 UPS
			SIST. CONTROL PERSONAL	1 ANTENA DE INTERNET

			SISTEMA DE GARNTIAS	1 COPIADORA
			CORREO ELECTRONICO	1 FAX
SOCK SHOP	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
PONDARMAT	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
PANBOEC	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	
TRENSAD	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
ECUADOR			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	1 FAX
BAKERY CIA.	2	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	
COORP STARS	3	2	WINDOWS XP	1 LINEA TELEFÓNICA
			MS OFICCE	1 ROUTER
			SISTEMA DE INVENTARIOS	1 SWITCH
			SISTEMA CONTABLE	

3.1.7 Planificación

Es la etapa donde se define y prepara el esfuerzo de planificación de contingencia y el Plan de Continuidad. En esta etapa además se incluye: Integración del Grupo de Trabajo para el Plan de Contingencia, adicionalmente el personal clave que será seleccionado un representante de cada uno de los almacenes los cuales serán identificados y registrados con su dirección, teléfono, y la empresa a la que representan. ***El día 2 de Junio de 2009 se dio inicio formalmente al desarrollo del Plan de Contingencia Informático, con la participación de personal administrativo del Conjunto de Bodegas PARKENOR, definiendo la necesidad de contar con un Grupo de Trabajo para la Coordinación de su desarrollo, mantenimiento y afinación.*** El Sr. Fabián Ruiz administrador del conjunto industrial, propuso la integración del Grupo de Trabajo involucrando a las siguientes personas:

Tabla 3.4: Grupo de trabajo para contingencias del Conjunto de Bodegas PARKENOR

ROLES	PUESTO	OCUPANTE ACTUAL
Presidente del Grupo de Trabajo	Presidente de PARKENOR	Presidente PAKENOR
Coordinador General	Administración de PARKENOR	Sr. Fabián Ruiz F.
Coordinador	Secretaría de la administración	Sra. Marcia Morales
Coordinador de Redes y Comunicaciones	Administrador de Redes y Comunicaciones	Sr. Romel Lara S.
Coordinador de Soporte Técnico	Soporte Técnico	Sr. Romel Lara S.
Personal Clave	Administradores de almacenes	

Tabla 3.5: Personal clave para contingencias del Conjunto de Bodegas PARKENOR

ALM.	NOMBRE	DIRECCIÓN	TELEFONO
4	Isabel Bonilla	Juan Barrezueta N70-71 y Moisés Luna	2479-936 2479-621
5	COMANDATO	Av. 10 de Agosto y Naciones Unidas junto a la bomba de gasolina	
6	Susana Morales	Juan Barrezueta N70-71 y Moisés Luna	2267-451 2452-453
12	Marco Molina	Av. De los Shyris 2317y el telégrafo	2252-725 2433-585
13	Olga Robalino	9 de Octubre y roca Ed. Santa Teresita	2527-139
15	Javier Sarango	Av. De los Shyris y República 2do piso	2262-728 ext. 2072
16	Edgar Aldas	Wandemberg E6-160 y Botadano	2810-165 2409-443
18	Portilla Charvet Javier Eduardo	República del Salvador 836 Ed. Prisma Norte piso 7 Ofic. 74	2550-590 2550-540 2260-710 099800830 099440266
19	Eugenia Camacho	San José y segunda trasversal 3 pisos	3260213 096010308
20	Sr. Fabián Castro	Manuel Larrea 311 y Arenas	2564-550
22	Agustín Yépez	Gonzalo Gallo OE-91 308 y Serrano	2240-536
1	Roberto Juriss	Gonzalo Gallo OE4-91y Manuel Serrano	2435-529 098939170
44	Sonia Valencia	Murgón 384 y Ulloa	2524-666
2	Víctor Jiménez	Ulloa 650 y Marchena	2230-199
60	Carlos Torres	Ed. Unicornio piso 11	2463-623 2467-616
76	Texaco Petroleum Company (Arrendatario)	Rumipamba E2-209 y Av. República Edificio Borja Páez 1 Piso Ofic. 12	Sr. Diego Borja 2262-709 / 2921-810 097695349
44	Francisco Calisto (Pablo Hidalgo)	Reina Victoria N25-33 y Av. Colón Ed. Banco de Guayaquil 4to piso Of. 405-A-B	2504-477 2569-832 099691204
16	Gilberto Tenesaca		2390-322 2391-851 ext. 104
19	Mundy Home	Tomas de Berlanga E4-85 Y Amazonas	2258-798 2258-799
22	Justo Prieto	Av. Marchena OE-256 y Versalles.	2505-966 2224-534
25	Sr. Cristian Vaca	Gregorio Bobadilla N36-24 y NNUU	2277-105 Cel. 096527063
23	Fernando Calvache	En Colombia	00573006088423 /
29	MECADEC	Av. Amazonas 4080 y Naciones Unidas	2261-767 2261-768

	(Arrendatario)	Edif. Puerta del Sol Torre	
30	Leonor Álvarez	Gonzales Suárez 869 Ed. Casa Bella	2362-036 2363-732
31	Eduardo Cordero	Mariano Echeverría OE-443 y Brasil	2483-735 099738180
32	BANRED (Arrendatario)	Av. 9 de Octubre N19-33 Edificio ETECO Piso 6 (El Ejido, frente al Banco Internacional)	Srta. Karina Tamayo 2502-018 fax 2238-884
35	Byron Checa	Pasaje Yaupi y Mariana de Jesús	2562-123 2562-124
33	Jorge Estrella	Julián Arbaiza E7-69 (Lote 10) y Pedro Cornelio	2411-724 2813-131 2404-789
35	Jorge Robalino	Calle Boyacá 161 y Av. Universitaria Sector Miraflores Casa 19-61	fax 2567610 098301088
36	Jorge del Salto	Las Avellanas N67-4	2801-123 099708038
39	Patricio Vascones	Guayaquil	042434354
40	Nicolás Gallardo	Wimper y Orellana	2905-290 2905-289 2223-554
41	Víctor Chiriboga	Av. 6 de diciembre 2816 y Paul Rivet	2222-600 2222-601
42	Cyede	Luis Cordero e Isabel la Católica esquina	2231-322 ext.121 2507-961
43	Byron Amores	Av. 6 de Diciembre 5247 y el Telégrafo Ed. García Ayala No.- 2	(2564-530)
107	Marcelo Moran	Guayaquil (Colón 535 y Av. 6 de Diciembre.	042492-670 (099721063 Moran) 099721063 / 094060414
115-	Hernán López	Japón y Pereira Lote No.- 3	2267-268 2270-271
	Guillermo Herrera	Mariano Aguilera E7-36 y la Pradera	2506-349 2506-353 2552-478 099721523
120 - 122	Fabián Echeverría	Av. República y la Pradera	2227-700 ext. 2110
98	Juan Serrano (Liquidador)	Av. 6 de Diciembre y Colón Ed. Parkenor 9no piso Ofic. Cife	2200-277 099257528

3.1.8 Definición de una estrategia de Planificación de Continuidad del Negocio.

El Conjunto de Bodegas PARKENOR ha desarrollado su Plan de Continuidad el cual se incluye dentro del Plan de Contingencia. Ver anexo 1.

El plan debe ser ejecutado independientemente de las operaciones y procedimientos operativos normales.

Si ocurre un desastre, una interrupción, o un desfase de gran magnitud en los negocios de la empresa durante el período del calendario de eventos, se pondrán en práctica los Planes de Continuidad de Negocios o de Contingencia.

- La Continuidad de los Negocios no cubre los Planes de Recuperación de Desastres que ya fueron emitidos.
- No se cubrirá el estudio de Pérdidas y Ganancias

3.1.9. Conceptos Generales

3.1.9.1 Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

3.1.9.2 Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

3.1.9.3 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos

3.1.9.4 Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

3.1.9.5 Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

3.1.9.6 Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

3.1.9.7 Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

3.1.9.8 Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

3.1.9.9 Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

3.1.9.10 Golpes

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

3.1.9.11 Definición de Roles.

3.1.9.11.1 Presidente del Grupo de Trabajo.

Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir los comunicados de concientización y solicitud de apoyo a los administradores y/o gerentes de las diferentes áreas involucradas y aprobar su culminación.

Una vez concluida la realización del Plan de Contingencia, el Presidente tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento del Plan de Contingencia Informático, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten.

Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizará las inversiones a realizar así como el fondo de efectivo a asignarse para los gastos necesarios.

El presidente se mantendrá permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión.

3.1.9.11.2 Coordinador General.

Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan de Contingencia, registrará las reuniones que se

realicen, a manera de minutas, aprobará los procesos críticos y tipo de evento que abarcará el Plan de Contingencia y aprobará junto con el Presidente del Comité la terminación de cada una de las fases y la conclusión del proyecto.

1. Establecer un Grupo de Trabajo y definir roles.

Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del plan. Al término de la realización de las pruebas, será el Coordinador General quién dé su Visto Bueno de la conclusión de éstas y de sus resultados, rindiendo un informe a todos los coordinadores involucrados y en general al personal involucrado, y en caso necesario, convocar a la realización de una segunda prueba, corrigiendo previamente las fallas que se hubieran presentado. Una vez que se encuentre aprobado el Plan de Contingencia, será el Coordinador General quien lleve a cabo formalmente la declaración de una contingencia grave y de inicio formal de la aplicación del Plan de Contingencia, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades; será el responsable de dar por concluida la declaración de contingencia.

3.1.9.11.3 Coordinador de Redes y Comunicaciones.

Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, Servicios de Internet, Intranet, correo electrónico y red del Conjunto de Bodegas PARKENOR,

mantener actualizados dichos procedimientos en el Plan de Contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación.

Asimismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar a cabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de iniciar una posible contingencia, ya sea tipo parcial, grave o crítica.

El Coordinador de Comunicaciones es el responsable de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan de Contingencia Informático.

Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.

3.1.9.11.4 Coordinador de Soporte Técnico.

Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, unidades de CD, faxes, copiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones del Conjunto de Bodegas PARKENOR, es responsable de elaborar o coordinar con los usuarios los respaldos de información.

Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos en donde se procese lo

enunciado en el párrafo anterior, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático.

En caso que se declare alguna contingencia que afecte a los equipos y/o al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la mayor brevedad, con el objeto de no agravar el daño o se llegara a tener consecuencias mayores.

Para tal efecto debe participar en pruebas del Plan de Contingencia en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia.

3.1.9.11.5 Coordinador de Sistemas.

Será el responsable de determinar los sistemas Críticos del Conjunto de Bodegas PARKENOR, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Coordinador de Programación deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales Técnicos y de Usuario, resguardándolos fuera de las instalaciones

para su consulta y utilización al momento de solicitarse.

3.1.9.11.6 Personal Clave.

Es el responsable de la aplicación de los procedimientos que describa el Plan de Contingencia para cada una de las diferentes circunstancias o contingencias previstas y de reportar con la periodicidad que se indique en el plan, al Coordinador de su área y al Coordinador General, los resultados de la aplicación de alguna de las fases del plan. Coordinarán con el personal del Conjunto de Bodegas PARKENOR involucrado, la realización de las actividades contenidas en el Plan de Contingencia para la situación que se hubiera presentado y tratar por todos los medios que les sea posible el logro de los objetivos y asegurar la continuidad de las operaciones del Conjunto de Bodegas PARKENOR, disminuyendo el impacto de la contingencia al mínimo.

Darán aviso al Coordinador de su área, cuando a su juicio, las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. En caso de requerir de actividades complementarias para regresar a las actividades normales, especialmente cuando se trate de los sistemas informáticos del Conjunto de Bodegas PARKENOR, deberán incluir el plan de actividades que se deberá seguir para retornar a la situación normal.

3.1.9.11.7 Personal del Conjunto de Bodegas PARKENOR involucrado

El personal en general, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se estuviera presentado sea grave (incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes del Conjunto de Bodegas PARKENOR (el propio inmueble, equipos, documentación importante, etc.).

Con posterioridad a la crisis inicial, deberá apoyar a solicitud del Coordinador de su área y/o del personal clave del Plan de Contingencia, en la toma del inventario de daños, para lo cual deberá seguir las instrucciones generales que indique el propio Plan.

En forma alterna, deberá dar cumplimiento a las instrucciones que se incluyan en el Plan de Contingencia Informático para darle continuidad a las funciones informáticas críticas, siguiendo los procedimientos establecido, con la salvedad de que deberá, en forma creativa y responsable, adaptarlos a las circunstancias de limitación que represente el cambio de ubicación de las diferentes áreas involucradas en los procesos y la utilización de recursos de cómputo, mensajería, comunicaciones, etc., limitados.

Al declararse concluida la contingencia, deberá participar activamente en la restauración de las actividades normales del Conjunto de Bodegas PARKENOR, esto es, apoyar en la movilización de documentación, mobiliario, etc., a las instalaciones originales o al lugar que le sea indicado, hasta la estabilización de las actividades.

Cuando sea necesario, deberá participar en la capacitación del nuevo personal o del personal eventual que hubiera sido necesario contratar.

3.2 FASE 2: IDENTIFICACIÓN DE RIESGOS

El Conjunto de Bodegas PARKENOR es un grupo de almacenes que tiene un desarrollo físico y económico vertiginoso como también los riegos y amenazas, por esta razón se procedió a un análisis de riesgos y amenazas en la empresa y por consiguiente el desarrollo del plan de contingencia de la empresa.

Es necesario reconocer y reducir de riesgos potenciales que afecten a los productos y servicios; es por ello que se considera dentro de un Plan de Contingencia, como primer paso la Reducción de Riesgos, para favorecer el cumplimiento de los objetivos institucionales.

El análisis y evaluación de riesgos se desarrolla en 2 situaciones

- Para entidades que desarrollan Planes de Contingencias su plan de adaptación y no tienen soluciones adecuadas. Este tipo de empresas debe realizar los siguientes procesos.

  1 Evaluar el impacto de los procesos críticos.

  2 Valorar la certificación de los proveedores

  3 Privilegiar proyectos, eliminando aquellos que resultan extemporáneos.

  4 Detectar deficiencias ante cambios en los sistemas afectados.

  5 Guardar copias de información empresarial mediante convenios de soporte.

- Entidades que a la fecha no han tomado previsión.

  Para aquellas entidades que no están realizando Planes de Contingencia, el análisis y evaluación de riesgos consta de:

1 Realización un diagnóstico integral del Sistema de Información.

2 Elaborar una lista de Servicios afectados evaluando su importancia, magnitud del impacto, cuantificar con niveles A, B, C u otro.

3 Identificar todos los procesos de los servicios afectados.

4 Analizar sólo los procesos críticos de los servicios.

Los desastres y crisis son eventos que pueden inhabilitar a PARKENOR de proveer normalmente sus servicios a los usuarios internos y la atención al público en General, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención.

Identificación de Amenazas:

- Terremoto
- Incendio
- Inundación y humedad
- Corte de Energía
- Falla de la red de voz y datos
- Fallas en Hardware o Software
- Sabotaje o daño accidental
- Vandalismo y manifestaciones

Las operaciones de PARKENOR, pueden ser afectadas en menor o mayor medida por los distintos siniestros tanto naturales, accidentales o provocados. Tomando en cuenta los resultados del Análisis de Riesgos realizado para el Sistema de Administración de la

Seguridad de la Información y los riesgos residuales, se definieron los siguientes eventos para ser considerados dentro de este Plan de Contingencia Informático:

3.2.1 PRIORIDADES E IMPACTO DE RECUPERACIÓN.

Alta. Afecta directamente en las operaciones de PARKENOR y sus clientes, los sistemas informáticos son afectados directamente.

Media. Afecta de manera intermedia a las operaciones de PARKENOR y podría afectar las operaciones de los sistemas informáticos.

Baja. No repercute en las operaciones de PARKENOR y los sistemas informáticos trabajan con normalidad.

3.2.2 TERREMOTO

Sin pérdida o daños menores del edificio: El siniestro puede afectar únicamente parte de la estructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del edificio; el impacto que provocaría en PARKENOR sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

Con pérdida del edificio: La pérdida de las instalaciones afectaría gravemente a las operaciones de PARKENOR y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

Tabla 3.5: Amenaza de terremoto

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Terremoto / negación de servicio	Centro de cómputo	El centro de cómputo se encuentra en una región de alta actividad sísmica.	Media	Alto	72 %
2	Terremoto / Negación de servicio	Ruteadores, switches y firewalls	Funcionan con energía eléctrica.	Baja	Alto	36 %

3.2.3 INCENDIO

ÁREA DE SISTEMAS (CENTRO DE COMPUTO): Se tiene gran impacto en la información ya que los sistemas utilizados residen en los Servidores y dispositivos de comunicación localizados en el centro de Cómputo y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el sistema, configurar el Servidor y restaurar los respaldos para continuar trabajando.

Centro de Cómputo de Emergencia: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el Centro de Cómputo. En el caso de las primeras el impacto que tendría en PARKENOR es menor, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto.

Tabla 3.6: Amenaza de incendio

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Incendio / negación de servicio	Centro de cómputo	No hay extintores dentro del centro de cómputo.	Baja	Alto	45 %
2	Incendio / daño de equipo	Centro de cómputo	No hay extintores dentro del centro de cómputo.	Baja	Alto	45 %

3.2.4 INUNDACIÓN Y HUMEDAD

Puesto que es equipo electrónico el que se maneja dentro de la institución, una inundación severa dañaría los dispositivos irremediablemente deteniendo las operaciones de la misma totalmente.

Un daño grave correspondería a una inundación en el Centro de Cómputo, en tanto que una inundación parcial o limitada a parte de las instalaciones (no al Centro de Cómputo) podría sólo ocasionar un daño medio sí no va seguido de corto circuito.

Tabla 3.7: Amenaza de inundación humedad

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Agua /condensación	Centro de cómputo	No hay indicadores de temperatura y humedad.	Baja	Alto	18 %

3.2.5 CORTE DE ENERGÍA

Las operaciones informáticas de PARKENOR se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos.

Actualmente PARKENOR cuenta con una planta de energía con capacidad para re-establecer la energía inmediatamente después de la pérdida de luz.

La planta de energía tiene capacidad de 250 KW, (312.5 KVA), 0.8 FACTOR DE POTENCIA, 60 HZ., 1800 R.P.M., 220 VOLTS, para abastecer el centro de computo de forma ininterrumpida.

Los servidores se encuentran conectados a un UPS de capacidad 3KVA, para entrar inmediatamente después del corte de energía y evitar daños en los equipos.

Tabla 3.8: Amenaza de corte de energía

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Falla eléctrica / negación de servicio	Servidores	Funcionan con energía eléctrica.	Media	Alto	72 %
2	Personal técnico de mantenimiento / descarga electroestática	PC	Funcionan con energía eléctrica.	Baja	Bajo	8 %
3	Falla eléctrica / Negación de servicio	Ruteadores switches y firewalls	Funcionan con energía eléctrica.	Media	Alto	72 %

3.2.6 FALLAS DE LA RED DE VOZ Y DATOS

RED: Representa la columna vertebral de las operaciones de PARKENOR, si la red falla en su totalidad las operaciones se detienen con la consecuente falta del servicio informático.

APLICACIONES: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales de PARKENOR, ya que pueden ser reinstalados casi de inmediato.

Tabla 3.9: Amenaza vos y datos

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Personal técnico de mantenimiento / negación de servicio	Centro de cómputo	El cableado dentro del centro de cómputo no se encuentra debidamente ordenado.	Media	Alto	54 %
2	Hacker / cambio en la configuración	Access Points	Cualquier computadora puede conectarse a la red wireless.	Alta	Alto	80 %
3	Código malicioso / negación de servicio	Windows 2000 Server (1), Linux Red Hat y Windows 2000 Server	Todos los puertos del servidor están disponibles desde la red interna.	Alta	Alto	80 %

3.2.7 FALLAS EN HARDWARE O SOFTWARE

Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

Tabla 3.10: Amenaza de hardware y software.

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Personal técnico de mantenimiento / descarga electroestática	Centro de cómputo	No se cuenta con piso antiestático.	Media	Alto	36 %
2	Polvo / daño de equipo	Centro de cómputo	No está definido un periodo para realizar la limpieza del centro de cómputo.	Alta	Alto	81 %
3	Negación de servicio	Linux Red Hat	No se ha actualizado el kernel del sistema operativo.	Media	Alto	72 %
4	Negación de servicio	MySQL	No se ha actualizado la versión de la base de datos.	Baja	Alto	36 %
5	Hacker / Negación de servicio	Apache/PHP	No se ha actualizado la versión del servidor Apache y PHP.	Media	Alto	90 %

3.2.8 SABOTAJE O DAÑO ACCIDENTAL

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran repetición de procesos para la captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles.

Tabla 3.11: Amenaza sabotaje o daño accidental

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Personal técnico de mantenimiento / descarga electroestática	Servidores	Susceptibles a variaciones en voltaje.	Baja	Alto	30 %
2	Hacker / sabotaje	Centro de cómputo	El centro de cómputo tiene una ventana protegida con barrotes que da al exterior del edificio. El área externa alrededor de la ventana cuenta con una reja que es fácil de saltar.	Baja	Alto	45 %
3	Personal técnico de mantenimiento / Descarga electr.	Ruteadores, switches y firewalls	Susceptibles a variaciones en voltaje.	Bajo	Alto	30 %

3.2.9 VANDALISMO Y MANIFESTACIONES

Un intento de vandalismo ya sea menor o mayor, podría afectar a las computadoras, periféricos y servidores así como las comunicaciones. Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo pues podría dañar los dispositivos o periféricos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado a la ciudadanía.

A continuación se menciona en forma enunciativa una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el área informática, el cual registre todos los movimientos de entrada del personal.
- Instalar identificadores mediante tarjetas de acceso.
- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).

- Contar, ya sea bajo contrato o mediante convenio, con un centro de cómputo alterno de características físicas y equipo de cómputo adecuado para darle continuidad a las operaciones críticas de PARKENOR, aún en forma limitada de cobertura y de comunicaciones.

El paro total de las operaciones dentro de PARKENOR afectaría principalmente a los servicios que son proporcionados a la ciudadanía, así como también en los almacenes del conjunto industrial, no se podría llevar a cabo el mantenimiento y monitoreo del equipo informático, pues manifestantes bloquearían las entradas e impedirían el acceso para realizar cualquier operación.

Los principales conflictos que pudieran presentarse son:

En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.

Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de PARKENOR, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc. en un sitio alterno, ya que no contarían con copia de la información.

A continuación se menciona en forma enunciativa una serie de medidas preventivas en caso de presentarse un paro total de las operaciones.

- Determinar lugares especiales, fuera del centro de datos, para almacenar los respaldos y copia de la documentación de referencia.

- El personal clave del Plan de Contingencia Informático, se compromete a dar la alerta del paro total y sacar los respaldos de información fuera del edificio dentro de un tiempo límite antes de ser declarada la huelga.
- Personal del área informática debe prever un sitio alterno para continuar con las operaciones críticas. Asimismo, se deberá establecer un tiempo límite de espera de solución de la huelga como por ejemplo 24 horas con el fin de no afectar el servicio proporcionado al público en general, si después de este intervalo la huelga continuara, se determinará el lugar o lugares de reubicación alternos.

Tabla 3.12: Amenaza sabotaje o daño accidental

N°	Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total
1	Manifestaciones / Falta de personal	Fabián Ruiz, Marcia Morales, Fernando Barrón, Liliana Morales	Ausentarse a laborar.	Media	Alto	60 %

3.3 FASE 3: IDENTIFICACIÓN DE SOLUCIONES

Un plan de contingencias debe contemplar todos los procesos institucionales sean estos manuales y/o automatizados, evaluando el volumen de información o materiales afectados, a fín de definir la complejidad de los sistemas. La magnitud, de un plan de contingencia será proporcional a la complejidad, importancia, costo del servicio al cual está destinado a proteger y el riesgo asociado a la misma.

El esquema general del plan de contingencias de los sistemas de información, está constituido por 3 grandes fases:

1 Fase de Reducción de Riesgos

2 Fase de Recuperación de Contingencia

3 Fase de Organización de un Sistema de Alerta contra Fallas

Se debe tener en cuenta al determinar los objetivos, en qué parámetros generales se va a basar, para poner en operación el plan de contingencias.

En cualquier caso, sus planes deben identificar dependencias e impactos y, al mismo tiempo, los recursos necesarios para implementar cada alternativa de contingencia.

En la siguiente tabla se muestra la matriz del plan de contingencia.

Tabla 3.13: Identificación de soluciones

OPCIONES	OPERACIÓN MANUAL	REEMPLAZO	SERVICIO EXTERNO
Reparación parcial	Use hojas de cálculo o base de datos para ofrecer alguna de la funcionalidad original del sistema (fecha de captura).	Tenga disponible software de repuesto que cumpla con los requisitos	Use personal temporalmente para llenar brechas
Reparación total	Ofrezca operaciones totalmente funcionales a través del proceso manual, utilizando personal adicional si es necesario	Use base de datos o paquetes para reemplazar la funcionalidad del sistema	Haga que el contratista procese los pagos en sus propias instalaciones
Reparación rápida y de defecto	Recurra al proceso manual sólo en caso de clientes prioritarios. Asegure que contará con personal el 1 y 2 de enero.	Elimine esfuerzos de reparación e implemente un sistema comercial funcional, rápidamente	Entregue el manejo de la plantilla de pago a una firma comercial especialista

3.3.1 IDENTIFICACIÓN DE ALTERNATIVAS

Como indicamos anteriormente, un buen método para identificar alternativas consiste en revisar los planes de administración de emergencia o recuperación de fallas. Estos son algunos ejemplos de alternativas que pudieran ayudarle iniciar el proceso de preparación.

- Planifique la necesidad de personal adicional para atender los problemas que ocurran.
- Recurra al procesamiento manual (de facturas, órdenes, cheques, etc.) si fallan los sistemas automatizados.
- Planifique el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
- Instale generadores si no tiene acceso a la red de energía pública.
- Disponga del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.
- Disponga de bombas manuales de combustible y úselas si fallan las electrónicas.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal.
- No haga nada y vea qué pasa – esta estrategia es algunas veces llamada arreglar sobre falla.

3.3.2 IDENTIFICACIÓN DE EVENTOS ACTIVADORES

Cuando el equipo de planificación seleccione la mejor alternativa de contingencia, debe definir los activadores que provocarán la implementación del plan. Los activadores son aquellos eventos que permitirán decir “OK”, es el momento de pasar al plan B”.

Incluyen las fallas de los sistemas, u otros eventos que hacen evidente la necesidad de implementar el plan de contingencia. Sin embargo, muchos eventos activadores serán predefinidos como puntos de decisión “pasar/no pasar”, el evento que active la decisión de poner en funcionamiento el proceso alternativo puede ser una alerta establecida a una falla anticipada.

La información necesaria para definir los activadores para cada sistema o proceso, provendrá tanto del programa de implementación para los sistemas de información, como de los requerimientos de tiempo desplegados para cada plan de contingencia.

A continuación se muestran algunos ejemplos de los tipos de eventos que pueden servir como activadores en sus planes de contingencia:

- Información de un vendedor respecto a la tardía entrega o no disponibilidad de un componente de software.
- Tardío descubrimiento de serios problemas con una interfaz.
- Tempranas (no anticipadas) fallas del sistema – corrección/reemplazo no está lista para sustituir.
- Fallas del Sistema (datos corruptos en informes o pantallas, transacciones pérdidas, entre otros).
- Fallas de interfaces e intercambio de datos no cumplen los requisitos.
- Fallo de la infraestructura regional (energía, telecomunicaciones, sistemas financieros)
- Problemas de implementación (por ejemplo, falta de tiempo o de fondos).
- Aseveraciones falsas o erróneas sobre el cumplimiento, descubiertas demasiado tarde para iniciar las acciones de cumplimiento.

Cabe mencionar que, para desarrollar este proyecto es necesario conocer los lineamientos generales del sistema afectado, es decir el tipo de producción al cual pertenece pudiendo pertenecer al sector de bienes o al sector servicios. Una vez establecido a que rubro de la producción pertenece, identificamos el departamento u área ligada y las funciones que en ella realiza, las áreas principales pueden ser:

- Contabilidad
- Administración
- Finanzas
- Comercialización
- Producción
- Seguridad

Se deberán identificar las fallas potenciales que puedan ocurrir para cada sistema, considerando la provisión de datos incorrectos, y fiabilidad del sistema para la institución, y así desarrollar una lista de alternativas priorizadas de fallas.

3.3.3 IDENTIFICACIÓN DE SOLUCIONES

El objetivo es reducir el costo, encontrar una solución en la medida de lo posible, a tiempo de documentar todos los riesgos identificados.

Actividades importantes a realizar:

- La asignación de equipos de solución para cada función, área funcional o área de riesgo de la organización.
- La asociación de soluciones con cada riesgo identificado- se recomienda tener un abanico de alternativas de soluciones, por que las soluciones se analizaran y se compararan posteriormente.

- Comparar los riesgos y determinar su importancia crítica en término del impacto de los mismos.
- Clasificar los riesgos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- La revisión de la factibilidad de las soluciones y las reglas de implementación.
- La identificación de los modos de implementación y restricciones que afectan a las soluciones.
- La definición e identificación de equipos de acción rápida o equipos de intensificación por área funcional o de negocios de mayor importancia.
- Identificar las soluciones y los riesgos y su importancia crítica en lo que respecta a su eficacia y su costo, siendo la meta la solución más inteligente.

La revisión de soluciones comparándolas con el nivel mínimo aceptable de resultados o servicios.

3.3.4 FALLAS COMUNES DE LOS SISTEMAS EN PARKENOR.

Se han encontrado varias fallas comunes en los sistemas informáticos en PARKENOR.

Estos incluyen:

Autentificación. Los usuarios no pueden determinar si el hardware y el software con que funcionan son los correctos. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

Cifrado. La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

Implementación. Un diseño bien pensado de un mecanismo de seguridad puede ser

implementado de forma improcedente.

Confianza implícita. Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

Compartimiento implícito. El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

Comunicación entre procesos. El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.

Verificación de la legalidad. El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

Desconexión de línea. En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualesquier recurso a los que tenga acceso el proceso.

Descuido del operador. Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

Paso de parámetros por referencia en función de su valor. Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una

situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad.

El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

Contraseñas. Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo (3) de intentos infructuosos.

Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

Privilegio. En algunos sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.

Confinamiento del programa. Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

Residuos. A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.). Las trituradoras de papel son algo corriente en ese aspecto.

Blindaje. Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles".

Valores de umbral. Están diseñados para desanimar los intentos de entrada, por

ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario (o el terminal desde donde se intentan las entradas) debe ser bloqueado y el administrador del sistema, advertido.

3.3.5 ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

Asincronismo. Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no es utilizado. Así, un proceso puede pasar valores erroneos a otro, aún cuando el segundo realice una verificación extensa.

Rastreo. Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

Entre líneas. Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

Código clandestino. Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.

Prohibición de acceso. Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

Procesos sincronizados interactivos. Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

Desconexión de línea. El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

Disfraz. El intruso asume la identidad de un usuario legítimo, después de haber obtenido

la identificación apropiada por medios clandestinos.

Engaño al operador. Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

Parásito. El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo.

Caballo de Troya. El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de sí mismo, después de la penetración.

Parámetros inesperados. El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

A medida que la computación se hace más asequible, los problemas de seguridad aumentan. Las comunicaciones de datos y las redes suponen un gran aumento de la vulnerabilidad de los sistemas basados en computadores. El hecho de ser favorables al usuario, implica también un incremento de la vulnerabilidad.

Los requisitos de seguridad de un sistema dado, definen lo que para ese sistema significa la seguridad. La seguridad externa se ocupa de la protección del sistema de computación contra intrusos y desastres. La seguridad de la interface del usuario se encarga de establecer la identidad del usuario antes de permitir el acceso al sistema. La seguridad interna se encarga de asegurar una operación confiable y sin problemas del sistema de computación, y de garantizar la integridad de los programas y datos.

La autorización determina qué acceso se permite a qué entidades. La división de tareas asigna al personal distintas responsabilidades. Ningún empleado tiene el control total de

las operaciones del sistema, y así comprometer la seguridad del conjunto industrial a varios empleados.

La vigilancia trata de la supervisión y auditoría del sistema, y de la autentificación de los usuarios. En la verificación de las amenazas, el sistema operativo controla las operaciones delicadas, y evitar el control directo a los usuarios. Los programas de vigilancia realizan operaciones sensibles.

Cuando los programas de vigilancia tienen un acceso mayor que los programas del usuario para servir las peticiones del usuario, se denomina amplificación.

3.3.6 SEGURIDAD EN REDES

3.3.6.1 Las Funciones de Seguridad de Red

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

- El intruso en la red.
- La autenticación de cliente y servidor.
- La autorización de cliente y servidor
- Contabilidad de cliente y servidor.

3.3.6.1.a. El intruso en la red.

El anfitrión adulterado es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.

3.3.6.1.b. Autenticación.

El procedimiento de acceso remoto es incierto, pues no se sabe si el usuario que ingresa es efectivamente quien dice ser, es por esto que se recomienda eliminar los accesos remostos hasta que el sistema sea eficiente y pueda controlar de una manera real el acceso de usuarios.

3.3.6.1.c. Autorización.

Aún cuando usted puede probar que usted es quien dice que es, simplemente, ¿Qué información debería permitir el sistema local revisar a través de una red? Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

3.3.6.1.d. Contabilidad

Finalmente, considerar el problema de contabilidad. Hay que recordar que nosotros debemos asumir que hay otros con un conocimiento mayor de sistemas. Cuánta contabilidad tiene que hacer el sistema para crear un proceso de respaldos. Este proceso debe ser periódico dependiendo de la cantidad de información que ingrese, puede ser diario, semanal o de acuerdo a las conveniencias del usuario.

3.3.7 COMPONENTES DE SEGURIDAD

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a

la red y copiar información fuera de ella, e incluso imprimirla.

Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se sugiere un sistema en tres niveles:

- **Nivel de administración.** Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.
- **Usuarios fiables.** Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.
- **Usuarios vulnerables.** Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones.

3.3.8 CONTROL DE ACCESO A LA RED

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Restringir las posibilidades de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.

- Protección con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en disquete en las estaciones de trabajo.

3.3.9 PROTECCIÓN DEL SERVIDOR

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlos de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

3.3.9.1 Redes y tolerancia a fallas

La tolerancia a fallas es la capacidad de la red de continuar funcionando, en el

caso que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente.

La tolerancia a fallas, se refiere no sólo a la redundancia, sino a la detección de errores. Por lo general, la tolerancia a fallas conduce a un elemento hardware redundante, que entra en funcionamiento de forma automática en el caso que el componente primario falle. Sin embargo la tolerancia a fallas puede ser algo como duplicar la FAT (tabla de localización de archivos) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras escritura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco.

No todas las redes requieren el mismo grado de tolerancia a fallas.

3.3.10 PROTEGIENDO LA RED

Estaciones de trabajo sin unidades 3.5 pulg., CD ROM. Una posible solución para poder impedir la copia de programas y datos fuera de la red en disquetes, y que a través de los disquetes ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin unidades de CD.

3.3.11 TECNOLOGÍA RAID

RAID (Arreglo Redundante de Discos Asequibles) reemplaza los sistemas de almacenamiento, grandes y costosos, con múltiples unidades de disco duro, pequeñas e idénticas. Potencialmente la tecnología RAID puede reducir el costo del almacenamiento, aumentar la velocidad y mejorar la confiabilidad del sistema.

El arreglo RAID sólo responde como un disco duro grande, en lugar de varios discos identificados por letras (en el caso de múltiples discos duros conectados a una computadora estándar). Más importante aún, el contenido de un archivo no está

concentrado en un sólo disco duro, sino que está esparcido a lo largo del arreglo, aumentando la seguridad de la información.

Sin embargo, esta seguridad tiene su precio. El precio por megabyte disminuye a medida que aumenta la capacidad del disco, por lo tanto un arreglo de discos menores inherentemente cuesta más que una unidad mayor de la misma capacidad total.

Además, los sistemas RAID pueden ofrecer a los usuarios de las redes, acceso a todos los datos, aunque un disco duro en el arreglo, falle catastróficamente.

Esta tecnología va más allá de los asuntos de confiabilidad para mejorar el rendimiento. Los múltiples discos en el arreglo pueden leer y escribir los datos en paralelo, dividiendo la información entre los discos a nivel de bit, byte o bloque, usando un proceso llamado la división de datos, y potencialmente pueden multiplicar la transferencia de información máxima por el número de discos en el arreglo.

Los controladores de discos avanzados pueden manejar múltiples peticiones simultáneamente, un método de búsqueda que reduce el tiempo de acceso a casi cero. Con este proceso, uno de los discos realiza la búsqueda mientras el sistema lee de otros discos.

3.3.11.1 Niveles De Raid

RAID viene en cinco niveles diferentes, los niveles del uno al cinco, cada uno diseñado para un uso específico. Estos números son simples designaciones de los diferentes métodos de proteger los datos en los discos duros y no describen los niveles de velocidad o calidad: RAID 1 no es mejor ni peor que RAID 5. El tipo de RAID apropiado para su servidor depende de cómo usa su red y el tipo de protección que desea proporcionarle.

RAID 1. Significa una redundancia total, dos discos de igual capacidad que duplican el contenido (o reflejan), uno del otro. Uno resguarda al otro automática y continuamente. El arreglo regresa a una operación de un solo disco si cualquiera de las unidades falla.

El Sistema RAID 1 está diseñado para los tipos de informaciones esenciales, cuyo reemplazo sería difícil y costoso. Aunque esta duplicación reduce la capacidad potencial de almacenamiento a la mitad, típicamente no tiene ningún efecto en el rendimiento. Sin embargo, los controladores RAID 1 sofisticados potencialmente, pueden duplicar el rendimiento leyendo sectores alternos de ambos discos.

RAID 2. Divide cada bit de los bytes o bloques de información entre discos separados y luego añade varios discos más para la corrección de errores. Por ejemplo, un sistema RAID 2 almacena una información digital de 16 bits en 16 discos, con 5 o 6 discos adicionales para la corrección de errores, o información de paridad. El número exacto de discos de corrección de errores que usa su sistema depende del algoritmo de división que se emplee. La penalidad en el tamaño del disco puede ser de hasta 37,5 por ciento, tres bits de corrección por cada ocho bits de información. Además, el diseño RAID 2 aumenta el tamaño de la unidad de almacenamiento mínima (el tamaño de los sectores se multiplica por el número de discos, un arreglo de 16 discos tiene sectores de 8.192 bits), haciéndolo ineficiente para almacenar archivos pequeños en tantos discos. Por otra parte RAID 2 logra razones de transferencia más elevadas porque los discos manejan los bits en paralelo.

Los errores se corrigen sobre la marcha, sin efectuar el rendimiento, porque el

controlador puede reconstituir la mayoría de los errores de la información redundante, sin tener que repetir la lectura de los discos duros.

RAID 3. Elimina parte de la minuciosidad que ofrece RAID 2, ya que utiliza la detección de errores en lugar de la corrección de errores. La detección de errores mediante el proceso de verificación de paridad requiere menos discos en el arreglo, típicamente uno por arreglo. Cuando el controlador detecta un error, hace que el arreglo vuelva a leer la información para resolver el problema. Esto requiere una revolución adicional en todos los discos del arreglo, lo que añade una pequeña demora en la operación del disco.

RAID 4. Los sistemas RAID 4, trabajan a nivel de sector en lugar de a nivel de bits. Los archivos se dividen entre los discos a nivel de sector, los sectores se leen serialmente, el primero de un disco, el segundo del próximo disco, y así sucesivamente. Para detectar errores, RAID 4 añade un disco dedicado a la paridad, mientras que el controlador de RAID 4 puede aumentar la velocidad con la división de datos. Se pueden leer simultáneamente dos o más sectores de discos diferentes, almacenarlos en RAM, que es mucho más rápida, normalmente varias órdenes de magnitud, y leerlos secuencialmente a la velocidad de la memoria.

Los mejores controladores de RAID 4 también procesan múltiples peticiones de datos simultáneamente, reorganizándolas, y luego leyendo los discos de la manera más eficiente, una tecnología conocida como búsqueda elevadora. Sin embargo, la escritura es más lenta que la lectura porque RAID 4 usa una tecnología de leer después de escribir. Después de escribir la información en el disco, se lee para determinar la paridad y escribir esa información en el disco de

paridad.

RAID 5. Elimina el disco de paridad dedicado de un sistema RAID 4. La información de paridad se añade como otro sector que rota por los discos del arreglo, exactamente igual a los datos ordinarios. Para un rendimiento mejor, los controladores de RAID 5 pueden añadir la división de datos y la búsqueda elevadora. Además, el sistema puede tener suficiente redundancia para ser tolerante a las fallas.

3.3.11.2 Ventajas y desventajas de la tecnología raid

- Dos tipos de RAID dominan los arreglos usados por las computadoras. RAID 1 es popular en los servidores de archivos NetWare, aunque Novell usualmente se refiere a esta tecnología como reflexión. Sin embargo, la mayoría de los dispositivos de computadoras llamados arreglos de discos, se adaptan al diseño RAID 5, ya que RAID 4 no ofrece ventajas reales, y RAID 2 y RAID 3 requieren demasiados discos y tienen demasiadas desventajas para ser útiles en la mayoría de las aplicaciones del entorno de la PC.
- Además de las capacidades extremas que se pueden obtener de los múltiples discos, la única ventaja que RAID ofrece a las computadoras de un solo usuario es potencialmente una mayor velocidad de transferencia. DOS usa entradas y salidas seriales (una petición de almacenamiento se debe satisfacer antes de emitir la otra), lo que no se beneficia de las búsquedas elevadoras.
- La confiabilidad adicional de un sistema RAID es una virtud dudosa cuando los discos duros ordinarios tienen clasificaciones MTBF (mean time between failures o tiempo promedio entre roturas) de 150.000 a 350.000 horas.

- Los servidores de archivos basados en PCs y la tecnología RAID, tienen sentido cuando se comparan a los sistemas de almacenamiento en los mainframes y minicomputadoras tradicionales: con discos duros del tamaño de refrigeradores de alta capacidad.
- La protección de la información que ofrecen los arreglos RAID, sustituye la solidez mecánica de las unidades de discos grandes, mientras logran una confiabilidad idéntica y en algunos casos superior.

3.4 FASE4: ESTRATEGIAS

Las estrategias de contingencia / continuidad de los negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

3.4.1 ACTIVIDADES IMPORTANTES

- La revisión de procesos, flujos, funciones y opciones de importancia crítica.
- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado (nivel de componente, nivel de proceso de la empresa).
- La revisión / depuración del cronograma maestro, incluyendo prioridades, fechas importantes en el calendario de eventos y dependencias cruzadas en diversos proyectos o áreas.
- La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes e identificar las estrategias globales.
- La identificación de los impactos de las soluciones y estrategias para ahorrar costos,

como puede ser la selección de una solución para cubrir varios riesgos, Se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución. Debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.

- La obtención de aprobaciones finales para el financiamiento, antes de que se apruebe la solución.
- La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto este equilibrado con los retornos reales de la organización.

3.4.2 IDENTIFICACIÓN DE SOLUCIONES PREVENTIVAS

Los puntos que deben ser cubiertos por todas las áreas informáticas y usuarios en general son:

- Respaldar toda la información importante en medio magnético, ya sea en disquetes, cintas o CD-ROM, dependiendo de los recursos con que cuente cada área. Acordamos que lo que debe respaldarse es información y no las aplicaciones.
- Generar discos de arranque para las máquinas dependiendo de su sistema operativo, ya sea WinXP o Win95, WinMe, Vista libres de virus y protegidos contra escritura.
- Mantener una copia de antivirus más reciente en disco para emergencias (dependiendo del fabricante, variarán las instrucciones para generarlo).
- Guardar una copia impresa de la documentación de los sistemas e interfaces, al igual de los planes de contingencia definidos por el resto de las áreas.
- Instalar todos los Service Packs que el equipo necesite y llevar un registro de los mismos, en caso de formatear el equipo o desinstalar aplicaciones.

3.4.3 MEDIDAS DE PRECAUCIÓN.

3.4.3.1 Área informática.

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Hasta hace algunos años la exposición de los equipos de cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de vandalismo y sabotaje.
- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.
- Otra precaución que se debe tener en la construcción del centro de cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al centro de cómputo debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de

trabajo, ya que un centro de cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.

- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de las claves y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- La seguridad de las terminales de un sistema en red podrán ser controlados por medios de anulación del disk drive, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.

- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.
- El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

3.4.3.1.1 Administración de los medios magnéticos:

- Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos.
- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

3.4.3.1.2 Administración de Impresoras:

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.
- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

***Niveles de Control*:**

Existen dos tipos de activos en un Centro de Cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del negocio, etc.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la

información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

En cambio tratándose de nivel clasificado, deben observarse además todas la medidas de seguridad de la información que estos equipos contengan.

3.4.3.2 Medios de Almacenamientos

3.4.3.2.1 Mantenimiento de Cintas Magnéticas y Cartuchos de tinta.

Las cintas magnéticas y cartuchos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada.

a. Cintas Magnéticas:

- La temperatura y humedad relativa del ambiente en que se encuentran almacenados deben estar en el siguiente rango:
- Temperatura : 4ºC a 32ºC
- Humedad Relativa : 20 % a 80 %
- El ambiente debe contar con aire acondicionado.
- Las cintas deben colocarse en estantes o armarios adecuados.
- Deberá mantenerse alejados de los campos magnéticos.
- Se les debe dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas que se hayan registrado sobre ellas.

b. Cartuchos:

- Temperatura : 16ºC a más
- Humedad Relativa : 20 % a 80 %
- La temperatura interna del Drive puede oscilar entre: 5ºC a 45ºC.
- Deben ser guardados dentro de su caja de plástico.
- Deben mantenerse alejados de campos magnéticos.

3.4.3.2.2 Recomendaciones para mantenimiento de Discos Magnéticos

Las recomendaciones para el buen mantenimiento de los discos magnéticos son:

- En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe.
- El cabezal de lectura-escritura debe estar lubricado para evitar daños al entrar en contacto con la superficie del disco.
- Se debe evitar que el equipo sea colocado en una zona donde se acumule calor, ya que el calor interfiere en los discos cuando algunas piezas se dilatan más que otras.
- Se debe evitar, en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

3.4.3.2.3 Recomendaciones para el Mantenimiento de los Discos Duros

Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

Se debe evitar que la microcomputadora se coloque en zonas donde haya

acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un Microcomputador.

3.4.3.3 Recomendaciones en los Monitores

La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.

Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.

Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.

También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.

Finalmente apague su monitor cuando no lo esté usando

3.4.3.4 Recomendación para el Cuidado del Equipo de Cómputo

Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

CPU. Mantener la parte posterior del CPU liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.

Mouse. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

Por Ejemplo:

Caso Epson FX-1170/LQ-1070 no usar rodillo cuando esté prendido.

Caso Epson DFX-5000/8000 tratar con cuidado los sujetadores de papel y no apagar de súbito, asegurarse que el ON LINE esté apagado, así evitaremos problemas de cabezal y sujetador.

Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

3.4.3.4.1 Mantener las Áreas Operativas Limpias y Pulcras

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas, para enunciarlas aquí. Sin embargo, algunos de los problemas que usted puede evitar son: el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche o chocolate en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo. Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza.

3.5 FASE 5: DOCUMENTACIÓN DEL PROCESO

Todo el proceso de lograr identificar soluciones ante determinados problemas no tendrá su efecto real sin la difusión adecuada de los puntos importantes que este implica, y un plan de Contingencia con mayor razón necesita de la elaboración de una documentación que sea eficientemente orientada.

Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

3.5.1 TERREMOTO

Análisis de daños:

En caso de daño mayor e imposibilidad de acceder al edificio:

Este tipo de procedimiento se tomará únicamente cuando el daño en el edificio haga imposible la continuación de las actividades, por lo que es preciso el traslado de las mismas a las oficinas consideradas como alternas (Instalaciones de la garita) o con el Proveedor correspondiente que proporcione dicho servicio.

Mientras las operaciones continúan en las instalaciones alternas, se evaluará la posibilidad de regresar a las instalaciones del Conjunto de Bodegas PARKENOR, ó establecer operaciones en un nuevo sitio.

Procedimiento.

Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones.

Restaurar la información de las bases de datos y programas.

Revisar y probar la integridad de los datos.

Iniciar las operaciones.

Desarrollar los procedimientos detallados de respuesta de emergencia.

En caso de daño menor:

Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.

Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.

Instalar el sistema operativo.

Responsable: Coordinador de Redes y Comunicaciones.

Restaurar la información de las bases de datos, y programas.

Revisar y probar la integridad de los datos.

Iniciar las operaciones.

La continuidad de las operaciones en este tipo de siniestros dependerá del grado de afección de la estructura del edificio, ya que las afecciones pueden ir desde el no daño de la estructura, daño parcial, hasta la inhabilitación completa del edificio.

Se considera daño mayor a toda aquella afección que imposibilite la utilización de los equipos y que ésta afección no tenga reparación ó bien por su naturaleza dicha reparación tarde un periodo prolongado.

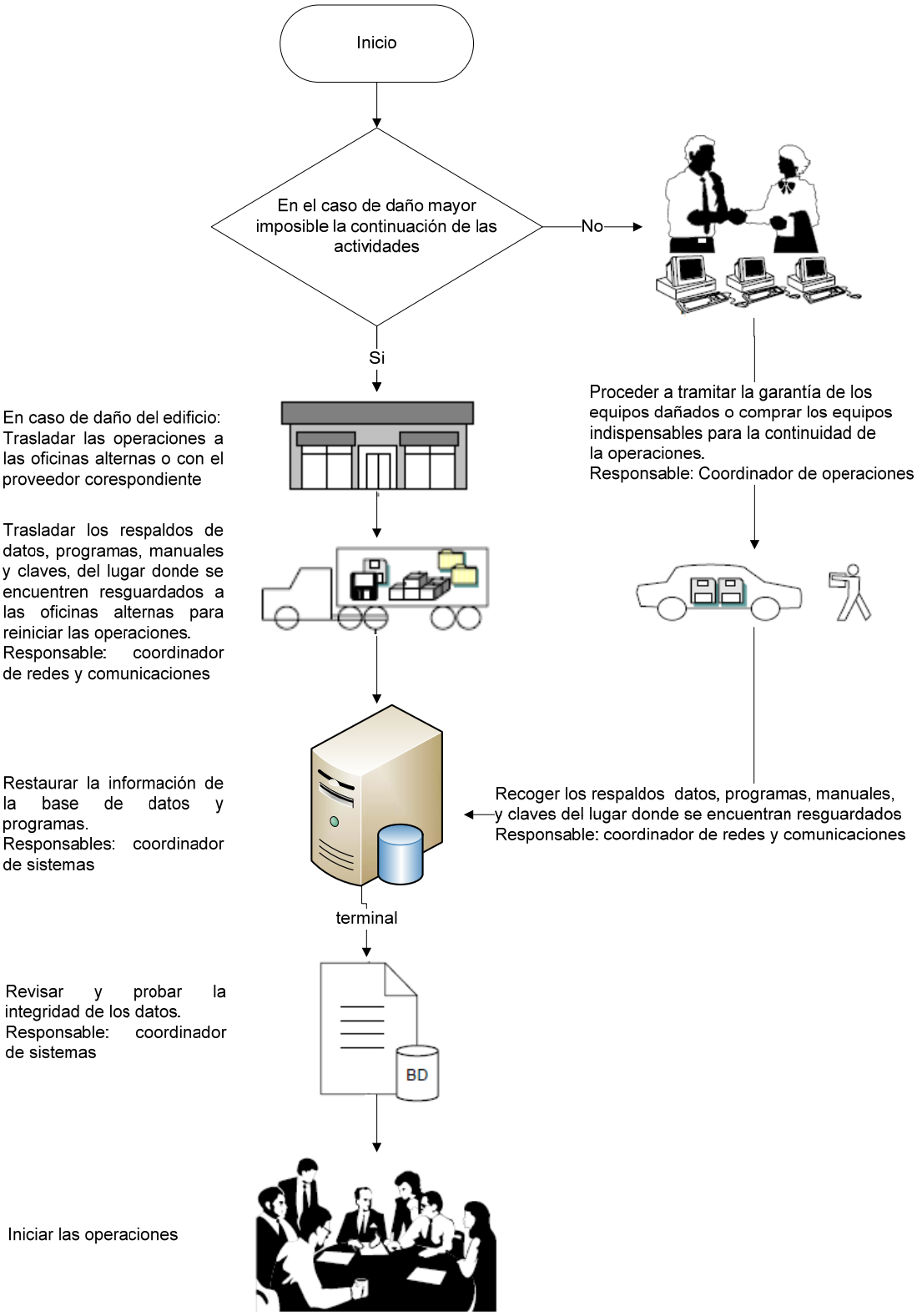

Figura 3.5.1: Diagrama de respuesta en caso de terremoto

3.5.2 INCENDIO

Análisis de daños

En caso de daño mayor e imposibilidad de acceder al edificio:

Este tipo de procedimientos se tomará únicamente cuando la reparación del edificio llegase a tardar mucho tiempo, durante este periodo de restauración se debe dar continuidad a las operaciones por lo que es preciso el traslado de las operaciones a otras oficinas.

Mientras las operaciones continúan en otras oficinas, se evaluará la posibilidad de regresar a las instalaciones del Conjunto de Bodegas PARKENOR ó establecer operaciones en un nuevo sitio.

Asimismo, los responsables del grupo de Trabajo del Plan de Contingencia Informático, deberán reunirse a la brevedad con el Presidente del Grupo de Trabajo, con el objeto de hacer un recuento rápido de los daños, determinar si es posible o no continuar utilizando las instalaciones y/o por cuánto tiempo aproximadamente se deberá operar fuera de las instalaciones o si la emergencia afectará solo a una parte del edificio.

En esa reunión se determinará la ubicación o ubicaciones alternas que ocupará cada una de las áreas y la manera como se llevará a cabo la coordinación y control de las operaciones del Conjunto de Bodegas PARKENOR.

Procedimiento.

- Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones.

- Restaurar la información de las bases de datos y programas.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

En caso de que durante el evento hubiera ocurrido algún accidente y se contara con personal afectado físicamente y que por tal motivo no pudiera continuar prestando sus servicios por algún tiempo, o en forma permanente, deberán tomarse las decisiones correspondientes y comunicarlas al personal involucrado.

Por lo que respecta a las operaciones del centro de cómputo, se continuará con la activación del Plan de Contingencia Informático, conforme al tipo de gravedad que se hubiere presentado, pudiendo inclusive, verse en la necesidad de iniciar los preparativos y ocupar las instalaciones alternas con el Proveedor correspondiente.

El responsable del área informática, deberá definir al personal que apoyará en la recuperación y retiro de los documentos, equipos y demás materiales importantes (cada área debe contar con una lista describiendo cada uno de ellos y la ubicación física en donde se encuentran), así como también deberá definir en conjunto con el Presidente del Grupo de Trabajo, si se contratará el servicio de mudanza o será con el personal y recursos de transporte propios quienes efectuarán la movilización, dependiendo de la cantidad de materiales a retirar.

Durante el retiro de los documentos, equipos, materiales, mobiliario, etc. importantes y necesarios para la continuidad de las operaciones del Conjunto de Bodegas PARKENOR, se deberá ir señalando en las listas aquellos documentos que se retiran (en cajas de preferencia), la persona que quedará como responsable de su transporte y el lugar de destino.

Lo anterior es importante para posteriormente estar en mejores condiciones de determinar el inventario final de pérdidas y daños de documentación importante, equipos, mobiliario, etc.

En caso de daño menor:

Procedimiento.

- Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
- Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
- Instalar el sistema operativo.
- Restaurar la información de las bases de datos, y programas.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

Es indispensable señalar que el daño en los distintos equipos puede variar desde el simple daño superficial hasta el daño permanente por lo que será necesario realizar la prueba de los equipos para poder determinar el grado de daño.

Se considera daño mayor a toda aquella afección que imposibilite la utilización de los equipos y que esta afección no tenga reparación ó bien por su naturaleza dicha reparación

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

1. Verificar periódicamente que las instalaciones eléctricas estén en perfecto

estado.

2. No debes concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.

3. Verificar las condiciones de extintores e hidrantes y capacítate para su manejo.

4. Si fumas, procura no arrojar las colillas a los cestos de basura, verifica que se hayan apagado bien los cigarrillos y no los dejes en cualquier sitio, utiliza ceniceros.

5. No almacenar sustancias y productos de fácil combustión.

6. No realizar demasiadas conexiones en contactos múltiples, evita la sobrecarga de circuitos eléctricos.

7. Por ningún motivo mojar las instalaciones eléctricas, recuerda que el agua es un buen conductor de la electricidad.

8. Al detectar cualquier anomalía en los equipos de seguridad (Extintores, hidrantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, repórtala de inmediato a la Coordinación de la Defensa Civil.

9. Mantener siempre el área de trabajo limpia y en orden.

10. Tener a la mano los números telefónicos de emergencia.

11. Portar siempre el gafete de identificación.

Antes de un incendio debemos estar siempre alertas, recordar que la mejor manera de combatirlo es la prevención.

DURANTE:

1. Si descubre un conato de incendio, actúe tranquilamente.

2. Si conoce sobre el manejo de extintores, intente sofocar el fuego; si éste es considerable no trates de extinguirlo con tus propios medios, solicita ayuda.

3. Si el fuego está fuera de control, realiza entonces una evacuación del inmueble, siguiendo todas las indicaciones del personal de emergencia.

4. No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No grite, No empuje, No corra y camine hacia la zona de seguridad.

5. Si hay humo donde te encuentras y no puede salir, manténgase al ras del piso, cubriendo su boca y nariz con un pañuelo bien mojado y respira a través de él.

6. Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.

7. Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

Tener presente que durante un incendio, el pánico es el peor enemigo.

DESPUES:

1. Retírese inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.

2. No obstruyas las labores del personal especializado, deja que los profesionales se encarguen de sofocar el incendio.

3. Personal calificado realizará una verificación física del inmueble y definirá si está en condiciones de ser utilizado normalmente.

4. Colaborar con las autoridades.

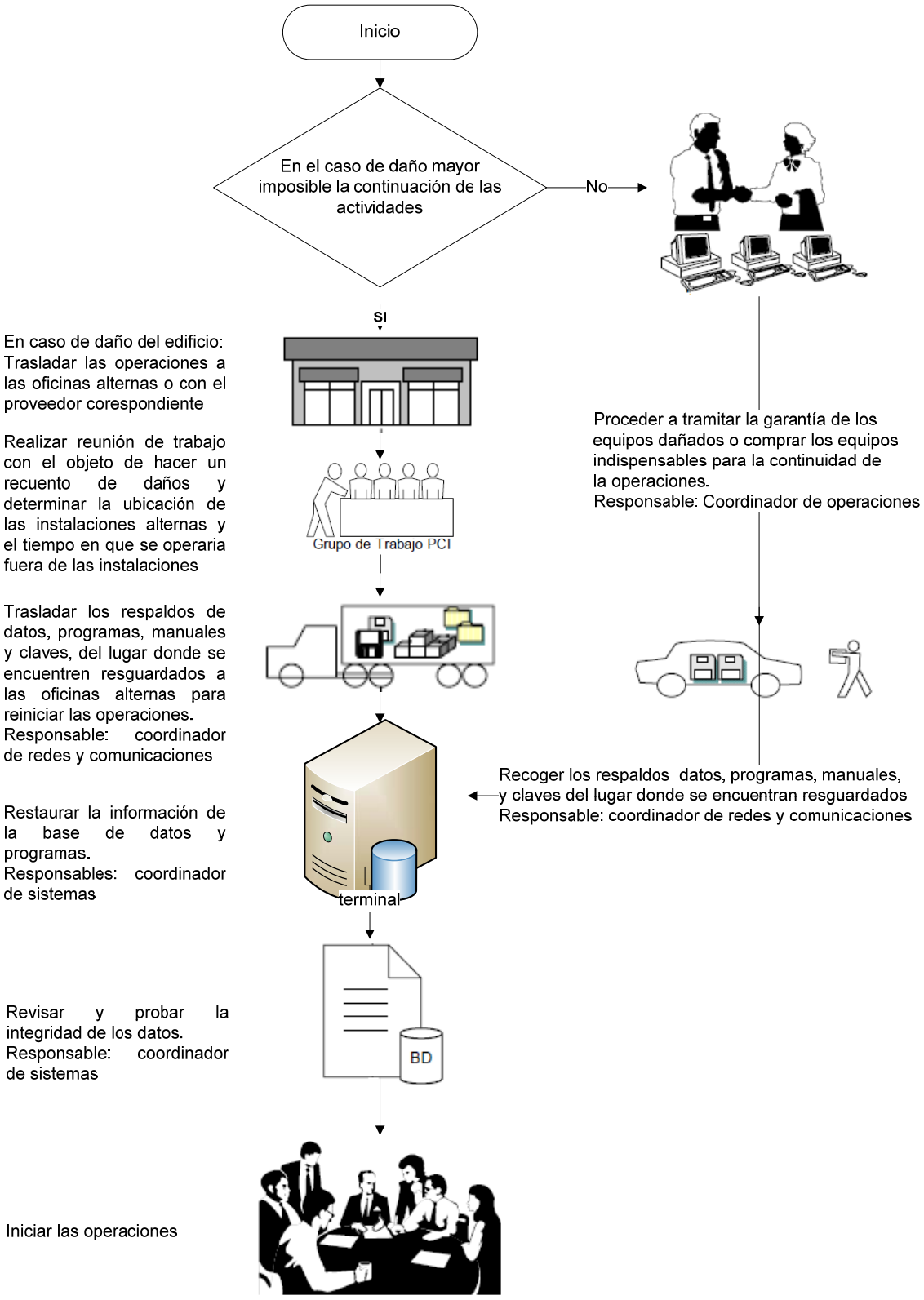

Figura 3.5.2: Diagrama de respuesta en caso de incendio

3.5.3 INUNDACIÓN

En caso de daño mayor:

Este tipo de procedimientos se tomará únicamente cuando el acceso a las instalaciones del Conjunto de Bodegas PARKENOR esté restringido y se tenga la certeza de que el daño en los equipos es irreversible.

Mientras las operaciones continúan en las instalaciones u oficinas alternas, se evaluará la posibilidad de regresar al Conjunto de Bodegas PARKENOR, ó establecer operaciones en nuevo sitio.

Así mismo, el Coordinador de PARKENOR, deberá reunirse a la brevedad con el Presidente del Conjunto de Bodegas, con el objeto de hacer un recuento rápido de los daños, determinar si es posible o no continuar utilizando las instalaciones y/o porque tiempo aproximadamente se deberá operar fuera de las mismas o si la emergencia afectará solo a una parte del edificio.

En esa reunión se determinará la ubicación(es) alternas que ocupará cada una de las áreas y la manera como se llevará a cabo la coordinación y control de las operaciones.

Los respaldos de información, serán custodiados fuera de las Instalaciones de PARKENOR, para lo cual se traslado y resguardo en las oficinas de presidencia.

Procedimientos a seguir.

- Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones.
- Restaurar la información de las bases de datos y programas.
- Revisar y probar la integridad de los datos.

- Iniciar las operaciones.

En caso de que durante el evento hubiera ocurrido algún accidente y se contara con personal afectado físicamente y que por tal motivo no pudiera continuar prestando sus servicios por algún tiempo, o en forma permanente, deberán tomarse las decisiones correspondientes y comunicarlas al personal involucrado.

Por lo que respecta a las operaciones del centro de cómputo, se continuará con la activación del Plan de Contingencia Informático, conforme al tipo de gravedad que se presente, pudiendo inclusive, verse en la necesidad de iniciar los preparativos y ocupar las instalaciones alternas.

El responsable del área, deberá definir al personal que apoyará en la recuperación y retiro de los documentos, equipos y demás materiales importantes (cada área debe contar con una lista y describiendo los mismos y la ubicación física en donde se encuentran), así como también deberá definir en conjunto con el Presidente de PARKENOR, si se contratará el servicio de mudanza o será con el personal y recursos de transporte propios del conjunto de bodegas quienes efectuarán la movilización, dependiendo de la cantidad de materiales a retirar. Durante el retiro de los documentos, equipos, materiales, mobiliario, etc. importantes y necesarios para la continuidad de las operaciones, se deberá ir señalando en las listas aquellos documentos que se retiran (en cajas de preferencia), la persona que quedará como responsable de su transporte y el lugar de destino.

Lo anterior es importante para posteriormente estar en mejores condiciones de determinar el inventario final de pérdidas y daños de documentación importante, equipos, mobiliario, etc.

En caso de daño menor:

- Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.
- Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren resguardados.
- Proceder (si lo amerita) al traslado de dichos datos al centro de respaldo u oficinas alternas con el propósito de reiniciar las operaciones.
- Instalar (sí lo amerita) el sistema operativo.
- Restaurar (si lo amerita) la información de las bases de datos, y programas.
- Revisar y probar de la integridad de los datos.
- Iniciar de las operaciones.

En caso de inundación las pérdidas pueden llegar a ser nulas, ya que el centro de cómputo debería encontrarse en una zona alta y no estaría expuesto a sufrir este tipo de daño.

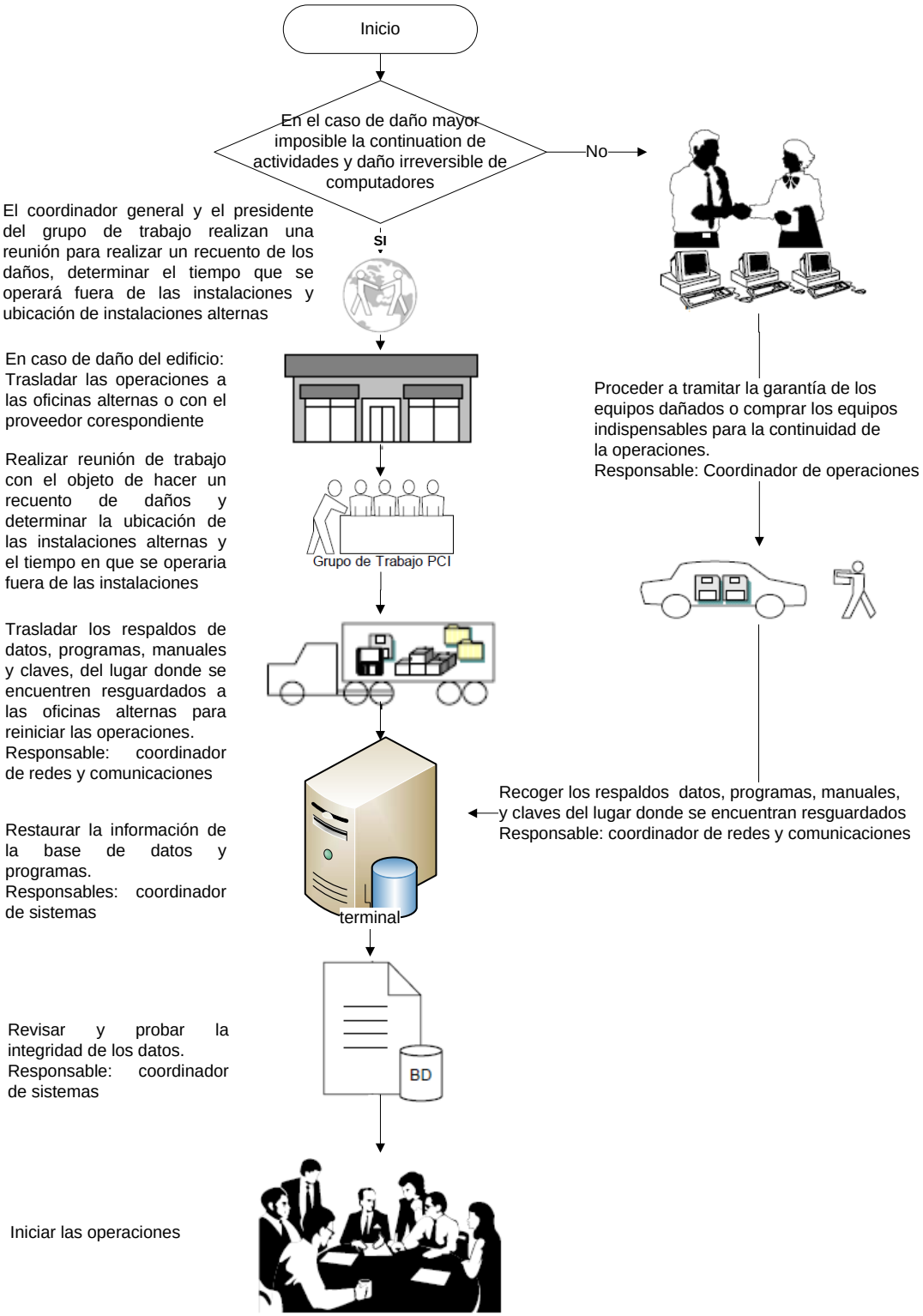

Figura 3.5.3: Diagrama de respuesta en caso de inundación.

3.5.4 CORTE DE ENÉRGIA

En el caso de cortes de energía, el Conjunto de Bodegas PARKENOR cuenta con una planta de energía la cual entra en funcionamiento inmediatamente, en el caso de que no entre automáticamente la planta, siempre se cuenta con la opción de encenderla manualmente.

Si por alguna razón la planta no funcionara se evaluaría el tiempo de reparación de la misma, si el tiempo de reparación excede de 72 hrs. o el corte de Luz dura más 8 hrs., se trasladaran las operaciones a las oficinas alternas.

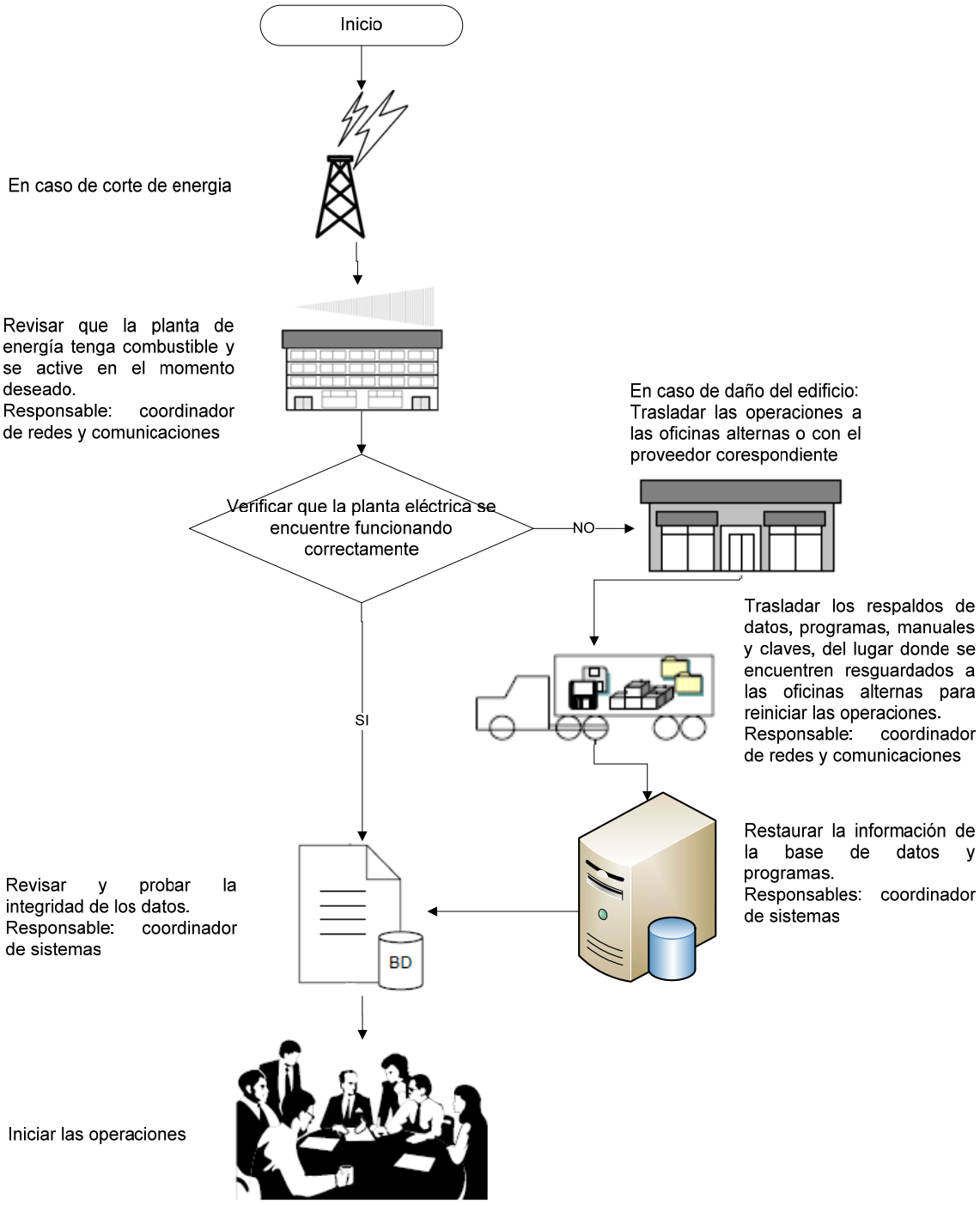

Figura 3.5.4: Diagrama de respuesta en caso de corte de energía

3.5.5 FALLA DE LA RED DE VOZ Y DATOS

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos ó a la pérdida de configuración de los mismos por lo que se deben evaluar las fallas para determinar si estas se derivan del mal funcionamiento de un equipo ó de la pérdida de su configuración. En este caso proceder de la siguiente manera

- Evaluación de las fallas.
- Si las fallas se derivan del mal funcionamiento de un equipo se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
- Si resulta ser un problema de configuración, se procede a su reconfiguración inmediata.
- Revisar y probar la integridad de las comunicaciones.
- Inicio de las operaciones.

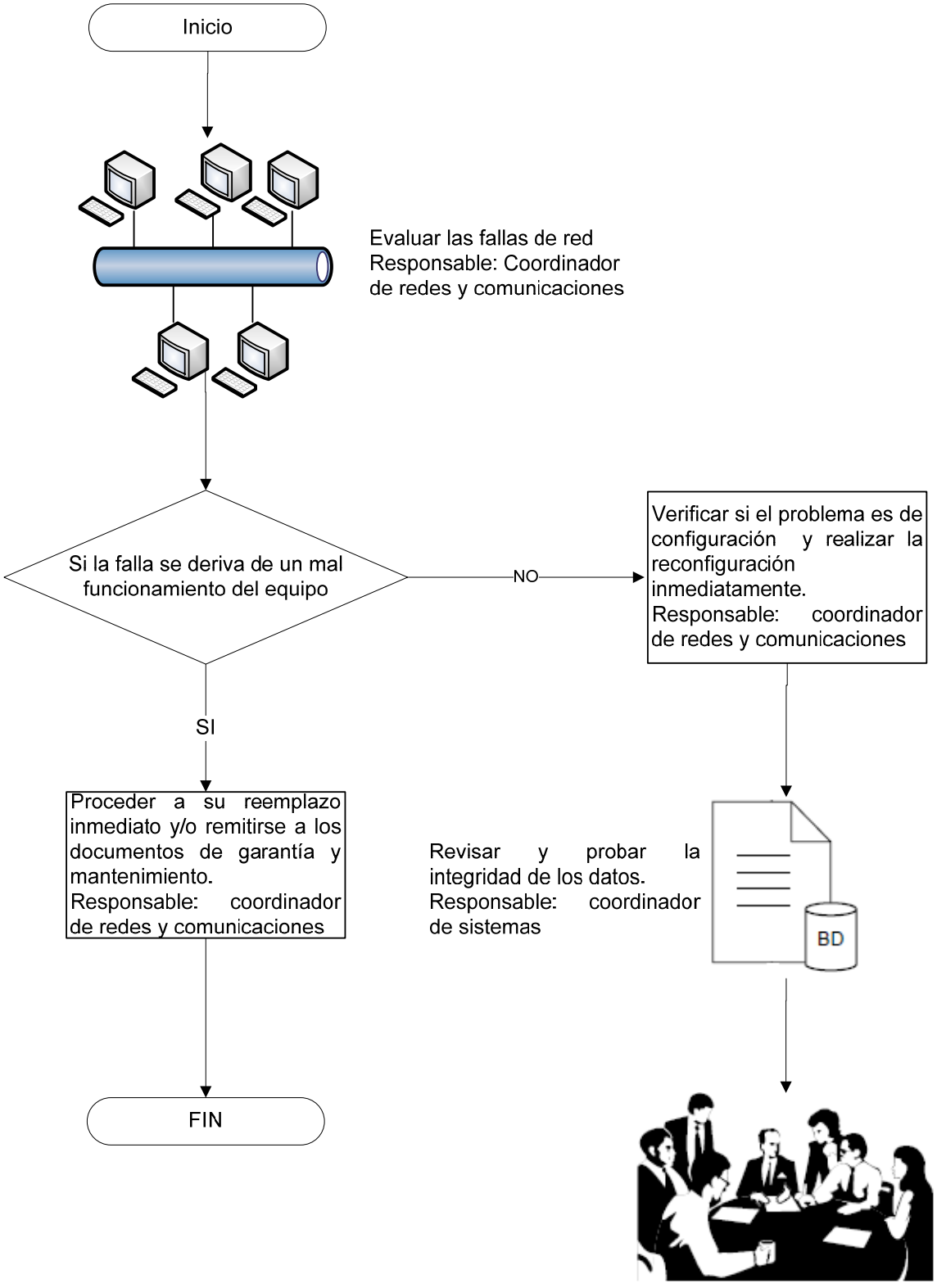

Figura 3.5.5: Diagrama de respuesta en caso de falla de vos y datos

3.5.6 FALLAS EN HARDWARE O SOFTWARE

En el caso que la alteración del hardware o el software en el Conjunto de Bodegas PARKENOR haga imposible el inicio inmediato o tardío de las operaciones se procede como sigue:

- Recoger los respaldos de datos, programas, manuales y claves del lugar en el que se encuentren resguardados.
- Si las fallas se derivan del mal funcionamiento de un equipo se procede a su reemplazo inmediato o remitirse a la póliza de mantenimiento.
- Instalar (sí lo amerita) el sistema operativo.
- Restaurar la información de las bases de datos y programas.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

Las alteraciones que sufran los servidores tanto en Software y Hardware pueden ser corregidas en la mayoría de los casos, sin embargo en algunas ocasiones, las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días sin tener la absoluta certeza de que las correcciones que se hicieron fueron las necesarias, por tal motivo es mejor acudir a los respaldos de información y restaurar los datos, de esta forma las operaciones del día no se verán afectadas y al mismo tiempo se ponen al día los datos faltantes de la operación del día anterior.

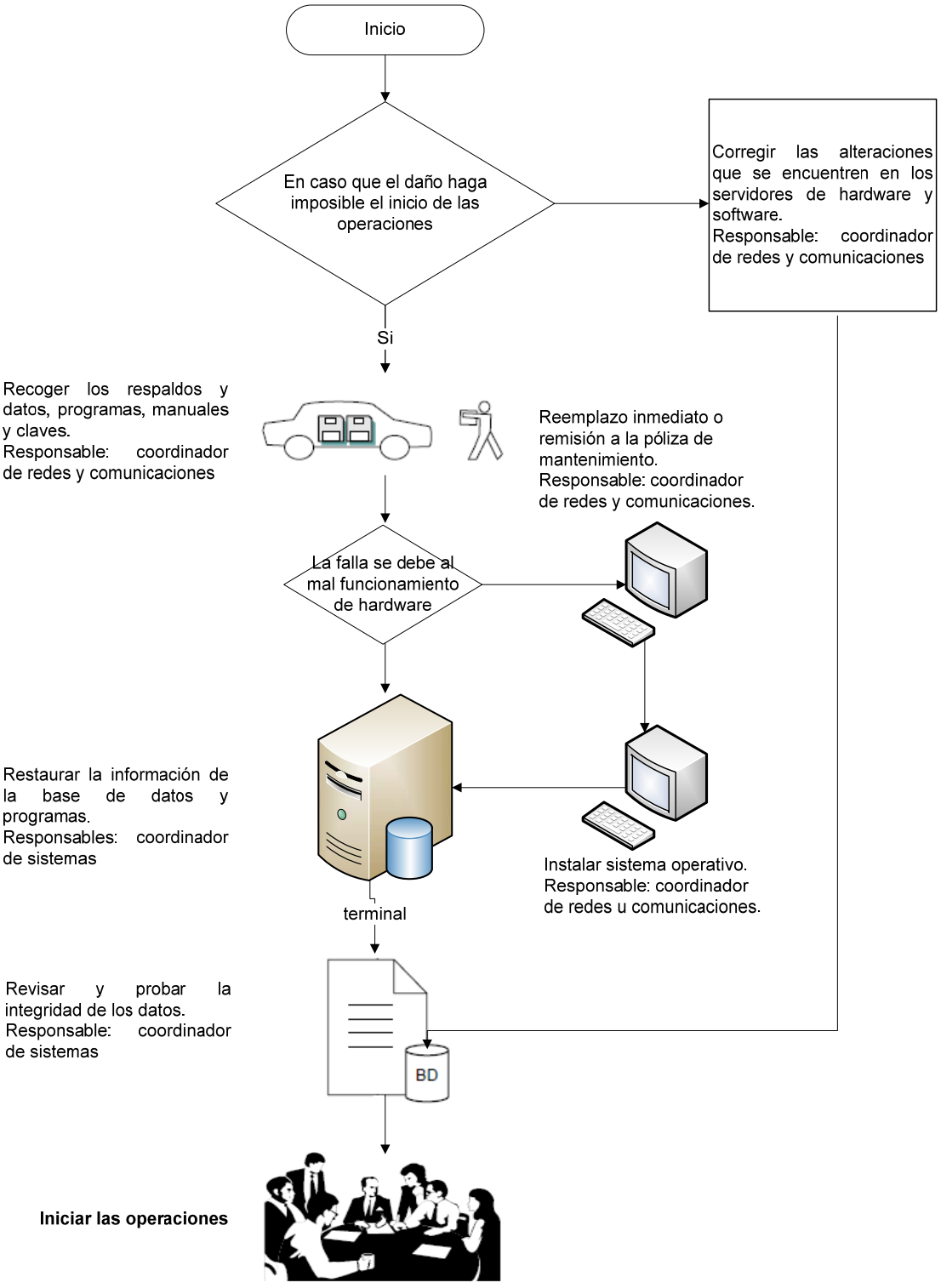

Figura 3.5.6: Diagrama de respuesta en caso falla en hardware y software

3.5.7 SABOTAJE Ó DAÑO ACCIDENTAL

Análisis y Evaluación de los daños ó pérdidas:

En el caso de que la eliminación haga imposible el inicio inmediato de las operaciones se procede con lo siguiente:

- Recoger los respaldos de datos, programas, manuales y claves del lugar en el que encuentren resguardados.
- Restaurar la información de las Base de Datos y Programas.
- Revisar y probar la integridad de los datos.
- Iniciar las operaciones.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse demasiado hasta por días, sin tener la absoluta certeza de que las capturas que se hicieron fueron las correctas, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectadas.

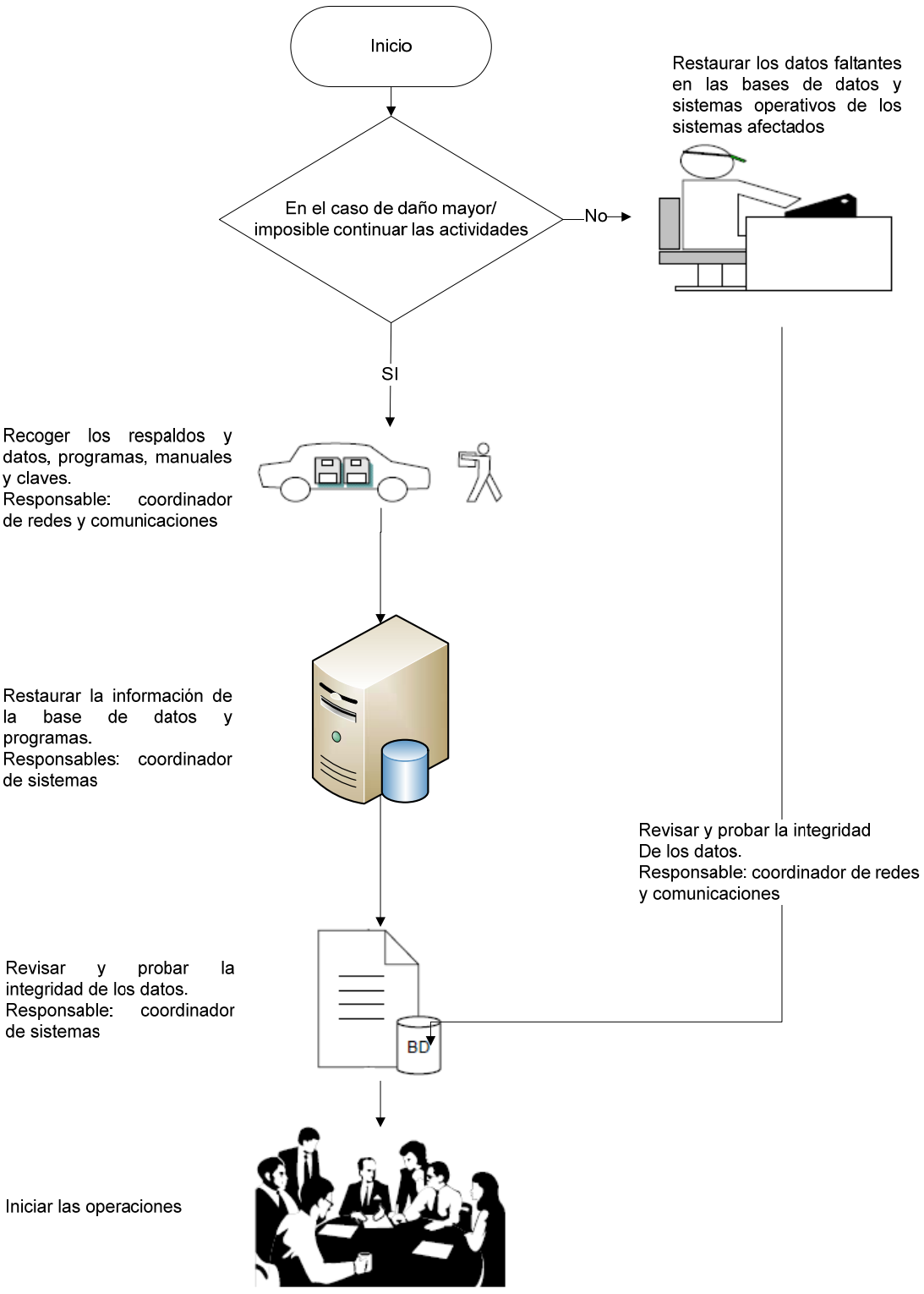

Figura 3.5.7: Diagrama de respuesta en caso sabotaje o daño accidental

3.6 FASE 6: REALIZACIÓN DE PRUEBAS Y VALIDACIÓN

3.6.1 PLAN DE RECUPERACIÓN DE DESASTRES

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

6.1.1.1 Actividades Previas al Desastre.

6.1.1.2 Actividades Durante el Desastre.

6.1.1.3 Actividades Después del Desastre.

3.6.1.1 Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren

un proceso de Recuperación con el menor costo posible a nuestra Institución. Podemos detallar las siguientes actividades generales:

3.6.1.1.1 Establecimiento de Plan de Acción

La fase de Planeamiento se debe establecer los procedimientos relativos a:

a) Sistemas e Información.

b) Equipos de Cómputo.

c) Obtención y almacenamiento de los Respaldos de Información.

d) Políticas de respaldo (Normas y Procedimientos de Respaldos).

3.6.1.1.2 Sistemas de Información.

PARKENOR deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).
- Las unidades o departamentos (internos/externos) que usan la

información del Sistema.

- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información

  Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

3.6.1.1.3 Equipos de Cómputo.

Aparte de las Normas de Seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

- Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.
- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador
- siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- Señalización o etiquetado de los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con información importante o estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada sistema permanente de la Institución (que por sus funciones constituyen el eje central de los servicios

informáticos de la institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

3.6.1.1.4 Obtención y Almacenamiento de respaldos.

- Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:
- Respaldos del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).
- Respaldos del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).
- Respaldos del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- Respaldos de los Datos (Bases de Datos, Índices, tablas de validación, claves, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

- Respaldos del Hardware. Se puede implementar bajo dos modalidades:

3.6.1.2 Actividades Durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

a) Plan de Emergencias.

b) Formación de Equipos.

c) Entrenamiento.

a) Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

Durante el día, durante la noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de

iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

b) Creación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c) Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

3.6.1.3 Actividad Después del Desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

a) Evaluación de Daños.

b) Priorización de Actividades del Plan de Acción.

c) Ejecución de Actividades.

d) Evaluación de Resultados.

e) Retroalimentación del Plan de Acción.

a) Evaluación de Daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

b) Priorización de Actividades del Plan de Acción.

Toda vez que el Plan de Acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola de acuerdo a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal en actividades que puedan no haberse afectado, para ver las actividades afectadas, en apoyo al personal

de los sistemas afectados y soporte técnico.

c) Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de PARKENOR o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

Evaluación de Resultados. Una vez concluidas las labores de recuperación del sistema que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro en sí, deben salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que

ocasionaron el siniestro.

d) Retroalimentación del Plan de Acción.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

3.7 FASE 7: IMPLEMENTACIÓN

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso hay que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

3.7.1 DE LAS EMERGENCIA FÍSICAS

CASO A: Error físico de disco de un servidor.

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último respaldo en el disco, seguidamente restaurar las modificaciones

efectuadas desde esa fecha a la actualidad.

7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Envía errores con mapas de direcciones hexadecimales.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de tarjeta(s) controladora(s) de disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Caso de incendio total

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

- Ante todo, se recomienda conservar la serenidad. Es obvio que en una situación de

este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO E: Caso de inundación

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
- Proveer cubiertas protectoras para cuando el equipo esté apagado.

CASO F: Caso de fallas de fluido eléctrico

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-Pass de corriente con el grupo electrógeno, previo aviso y coordinación.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

   ***** Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS. ****** Llámese corriente normal a la brindada por la compañía eléctrica.

   ******* Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

3.7.2 DE LAS EMERGENCIAS LÓGICAS DE DATOS

CASO A: Error lógico de datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

1. Caída del servidor de archivos por falla de software de red.
2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

3. Bajar incorrectamente el servidor de archivos.
4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de DOS, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: Caso de virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

1. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación

2. El antivirus muestra el nombre del archivo infectado y quién lo usó.
3. Estos archivos (.exe, .com, .ovl, .nlm, etc.) serán reemplazados del original de instalación o de los respaldos.
4. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red: Se revisará las computadoras que no estén en red con antivirus de disquete. De suceder que una computadora se haya infectado con uno o varios virus ya sean la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

Utilizar un disquete que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho disquete.

Retirar el disquete con el que arrancó el computador e insertar el disquete antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren.

3.8 FASE 8: MONITOREO

La fase de Monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo

o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero. Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar.

Podríamos enumerar las actividades principales a realizar:

1. Revisión de funciones y factores de riesgo.
2. Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.
3. Revisión periódica de las aplicaciones.
4. Revisión continua del sistema de respaldos
5. Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.

CAPÍTULO IV

DESARROLLO DEL PLAN DE CONTINGENCIA INFORMÁTICO DE LOS SISTEMAS DE INFORMACIÓN PARKENOR.

La implementación de un plan de contingencia establece 9 etapas en secuencia lógica que facilitan su desarrollo. (Ver Fig. 1)

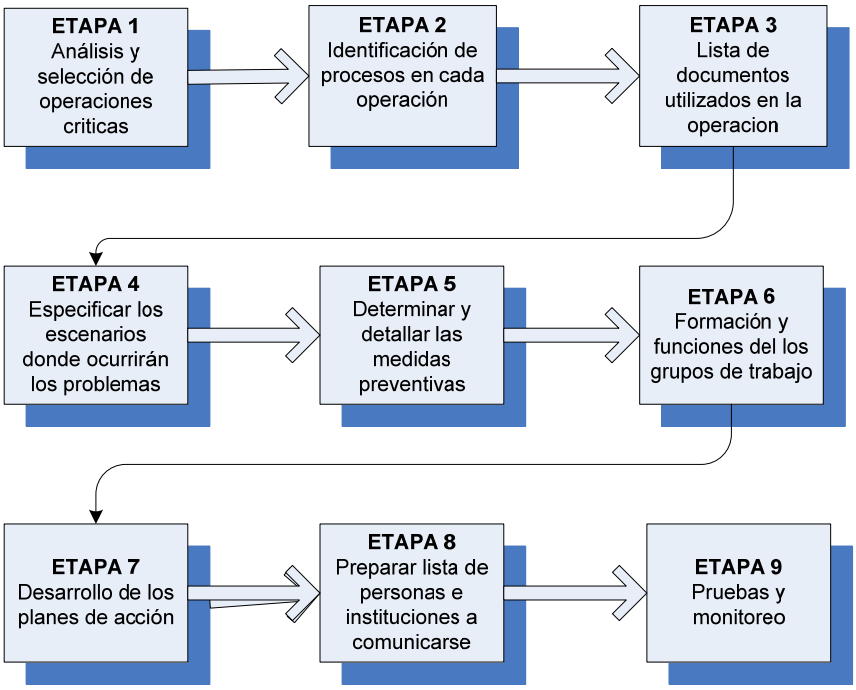

Figura No.4.1 "Etapas para el desarrollo de un Plan de Contingencia"

La figura No. 1 presenta en forma simplifica y grafica la secuencia lógica de etapas para desarrollar un plan de contingencia de los sistemas informáticos de una institución [4].

4.1 ANÁLISIS Y SELECCIÓN DE LAS OPERACIONES CRÍTICAS

Permite identificar cuáles serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información con los cuales estamos trabajando en PARKENOR, a continuación anotamos los más relevantes y los cuáles son:

- Datos
- Aplicaciones
- Tecnología Hardware y Software
- Instalaciones
- Personal.

Dentro de los nombrados podemos identificar varios pero que pueden variar de sistema a sistema:

- Reportes Impresos de Informes del Sistema.
- Acceso remoto a servidores de red.
- Consultas a las Bases de Datos vía Internet.
- Consultas a las Bases de Datos vía LAN.
- Sistema de Respaldos y Recuperación de Datos.
- Sistema de ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.
- Los Servidores de Bases de Datos y Aplicaciones.
- Los Servicios de Red.
- Los Medios de Transmisión.

- Las Topologías de Red.

Se ha listado los procesos críticos y evaluado su grado de importancia en función a la magnitud del impacto, y luego clasificados en niveles Alta, Regular y Bajo

A = Alta, **R** = Regular, **B** = Baja

Tabla 4.1: Operaciones criticas del sistema de información.

OPERACIONES CRÍTICAS	OBJETIVOS DE LA OPERACIÓN	PRIORIDAD DE OPERACIÓN
Reportes Impresos de Informes del Sistema	• Informes estados financieros • Informes de plantillas del personal. • Informes de producción mensual, anual.	R
Consultas a las Bases de Datos vía Internet	• Informes a los clientes. • Información a los proveedores. • Sistema de ventas vía Internet.	B
Consultas a las Bases de Datos vía LAN	• Inventarios • Revistas, electrónicas.	R
Sistema de respaldo y recuperación de datos	• Procesos de respaldos de la información. • Establecimiento de las frecuencias de almacenamiento de datos.	A
Sistema de Ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.	• Proceso de los programas que realizan la entrada y salida de la información. • Mantenimiento adecuado de las aplicaciones. • Equipamiento necesario para un funcionamiento optimo del sistema.	A

A = Alta, R = Regular, B = Baja

Tabla 4.2: Procesos estratégicos del negocio.

OPERACIÓN PRINCIPAL	CONTENIDO DE LA OPERACIÓN	PRIORIDAD DE OPERACIÓN
Ventas	• Ventas a los clientes	R
Ordenes aceptadas	• Aceptar órdenes de los clientes • Administración de las ventas a crédito	A
Envío y reparto	• Administración del inventario • Envío de productos Reparto de las ventas a crédito	A
Compra	• Dando órdenes a los fabricantes • Administración de la compra a crédito	A
Producción	• Fabricación	A
Estadísticas	• Estadísticas mensuales • Estadísticas anuales	R
Elaboración de informes de la administración	• Elaboración de reportes totales de Administración	B

Procesos relacionados a los usuarios y clientes en un proceso especifico de trabajo.

Tabla 4.3: Análisis sobre un proceso del negocio.

PROCESOS DE NEGOCIOS	RECURSOS USADOS	ORDENES ó NOTAS
Recepción de órdenes de pedido	Teléfonos fijos	Clientes
	PC´s	Clientes
	Líneas dedicadas	Usuarios
Confirmar la cantidad total límite de órdenes recibidas	Sistema de aceptación de la orden (Software)	Clientes
Confirmar si se cuenta con el Stock para atender los pedidos	Sistema de aceptación de la orden	Usuarios
Registrar las órdenes	Sistema de aceptación de la orden	Usuario
Enviar las confirmaciones de órdenes (faxearlas automáticamente)	Sistema de aceptación de la orden	
	Faxes	clientes
Indicar el envío o remitirlas a sus respectivos centros	Sistema de aceptación de la orden	clientes
	Líneas dedicadas	Grupos de Trabajo en los almacenes

Tabla 4.4: Lista de recursos utilizados.

RECURSO	UBICACIÓN	PROVEEDOR DEL SERVICIO
Computadores	Externo	PC PLUS
Software de Administración de contabilidad	Externo	PROVEEDOR PRIVADO
	Interno	SOPORTE TÉCNICO PRIVADO
Líneas dedicadas	Externo	C.N.T (ANDINATEL) PORTA CELULAR
Sistema de aceptación de orden (Software Base)	Interno	PC PLUS
	Interno	PC PLUS
Almacén automatizado	Interno	OFICINAS PARKENOR
Antenas de recepción	Interno	PROVEEDOR DE INTERNET
Servicio seguridad	Interno	SERRVICIO DE SEGURIDAD
Camiones internos	Interno	SERVICIO PRIVADO
Servicio de administración de bodegas	Externo	PROPIETARIOS
Servidores	Interno	ELECTRÓNICA B
Software Clientes	Interno	DESARROLLO INTERNO DE SEGURIDAD

Tabla 4.5: Lista de periodos aceptables de interrupción del hardware.

RECURSO	FRECUENCIA DE USO	PERÍODO ACEPTABLE DE INTERRUPCIÓN
PC´s (Red)	Cada día	Medio día
PC´s (no Red)	Cada día	Medio día
Software (Red)	Cada día	Medio día
Software de contabilidad	Cada día	Medio día
Software de vigilancia	Cada día	Medio día

Tabla 4.6: Lista de periodos aceptables de interrupción del software.

RECURSO	FRECUENCIA DE USO	PERÍODO ACEPTABLE DE INTERRUPCIÓN
Sistema de red	Cada día	Medio día
Líneas dedicadas	Cada día	Un día
Sistema contable	Cada 3 días	3 días
Línea Troncalizada	Cada día	Medio día
Sistema de contable	Cada día	Medio día
Sistema vigilancia DVR	Cada día	Medio día
Servidores	Cada día	3 horas
Software Cliente	Cada día	3 horas

Tabla 4.7: Lista de posibles problemas.

Recurso	Proveedor del servicio	RESULTADO CONFIRMADO	JUICIO DE COMPAÑÍAS	
		condiciones de preparación de las medidas preventivas	posibilidad del problema	periodo necesario para la recuperación
Servidores	Electrónica (Red)	Preparación de las medidas preventivas	Pequeña	3 Horas
Software	Desarrollo (Red)	Preparación de las medidas preventivas	Pequeña	3 horas
Clientes	Electrónica (Fax)	Equipos listos para los problemas de los sistema de información	Pequeña	3 horas
Líneas dedicadas	Teléfono (Red)	Preparación de las medidas preventivas	Pequeña	Medio día
Sistema de aceptación de orden (Software Base)	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	2 días
	Electrónica (Hardware)	Preparación de las medidas preventivas	Pequeña	5 días
Almacén del conjunto	Industrial	Preparación de las medidas preventivas	Pequeña	2 días
Elevadores del almacén	Industria pesada	Las partes que pueden tener problemas son reemplazadas y las máquinas examinadas	Pequeña	3 días
Servicio de reparto.	Transporte	Preparación de las medidas preventivas	Grande	2 días
Sistema de vigilancia DVR.	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	7 días

4.2. IDENTIFICACIÓN DE PROCESOS EN CADA OPERACIÓN

Para cada una de las operaciones críticas, se debe enumerar los procesos que tienen.

Niveles de riesgo: Crítico, No Critico

Tabla 4.8: Lista de procesos del área analizada.

RECURSO UTILIZADO	NIVEL DEL RIESGO
Sistema Eléctrico	Crítico
Red de Datos	Crítico
Servidores	Crítico
Sistemas de Gestión	Crítico
Impresoras	No Crítico
Humanos	No Crítico
Proceso de entrada y salida de la información	Crítico
PC's	Crítico
Sistema Eléctrico	Crítico
Teléfono	Crítico
Seguridad digital	Crítico
Contabilidad informática	No Crítico
Red de Datos	No Crítico
Mantenimiento adecuado de las aplicaciones	Crítico
Teléfono celular	No Crítico
Internet	Crítico
Servicio de seguridad	Crítico
Procesos Plan de Contingencia	Crítico

Los responsables de desarrollar los planes de contingencia deben de coordinar en cooperación con el personal a cargo de las operaciones de los Sistemas Analizados, los cuales son conocedores de dichos procesos críticos.

Se debe investigar los recursos administrativos (equipamiento, herramientas, sistemas, etc.) que son usados en cada proceso, se ha descrito y codificado cada recurso, como: sistema eléctrico, tarjetas, transporte, red de datos, PC's. A su vez también se ha determinado su nivel de riesgo, como críticos y no críticos.

4.3. LISTA DE RECURSOS UTILIZADOS POR LAS OPERACIÓNES

En esta etapa se identifica a los proveedores de los servicios y recursos usados, considerados críticos.

- Se tiene que identificar los recursos asociados al Sistema de Información.
- Se investiga y describe, si los recursos están dentro del Sistema de Información o fuera de este, (como compra a otros proveedores de servicios externos o productos).
- Se investiga y describe a los proveedores de servicios y recursos.
- La importancia de un mismo recurso difiere de operación en operación. Para esto se señala a que operaciones está relacionado el mismo recurso, esto es necesario para determinar las medidas preventivas para posibles problemas del Sistema de Información.
- Recurso
- Ubicación
- Proveedor del Servicio

Tabla 4.9: Lista de recursos críticos utilizados

RECURSOS PC´S/ (RED)	UBICACIÓN INTERNO	PROVEEDOR DEL SERVICIO
Software de Administración de vigilancia	Interno	Área de Soporte
Servidores internet, troncal, DVR,	Interno	Área de Soporte
Software de Gestión de órdenes (Software de los diferentes módulos que tiene la organización)	Interno	Área de Desarrollo de Software
PC's	Interno	Área de Soporte
Software Cliente	Externo	Proveedor
	Interno	Soporte Técnico

4.4. ESCENARIOS EN LOS CUALES PUEDEN OCURRIR LOS PROBLEMAS.

- En consideración de la condición de preparar medidas preventivas para cada recurso, se ha evaluado su posibilidad de ocurrencia del problema como (alta, mediana, pequeña).
- Se calcula y describe el período que se establecerá hasta la recuperación en caso de problemas, basados en información confirmada relacionada con los Sistemas de Información.

Mediante el siguiente cuadro podemos elaborar la Probabilidad de fallas de cada uno de los recursos identificados

Probabilidad: alta, mediana, pequeña.

Tabla 4.10: Lista de probabilidad de fallas de recursos.

Recursos	PROBABILIDAD DE FALLA DE RECURSOS		
	Alta	Media	Baja
Computadores			X
Internet		X	X
Línea telefónica		X	X
Línea troncalizada		X	X
Sistema de vigilancia digital	X		
Sistema contable		X	
Sistema eléctrico		X	

Mediante la siguiente tabla debemos priorizar los riesgos identificados tomando en cuenta el impacto del riesgo como la probabilidad de una falla en el área..

Impacto: Alto, medio, bajo

Prioridad de riesgos: Prioridad1, prioridad2, prioridad3

Tabla 4.11: Prioridad de atención de riesgos

I M P A C T O	PRIORIDAD DE ATENCIÓN DE RIESGOS			
	ALTO	Prioridad 3	Prioridad 3	Prioridad 3
	MEDIO	Prioridad 2	Prioridad 2	Prioridad 2
	BAJO	Prioridad1	Prioridad 1	Prioridad 1
		BAJO	**MEDIO**	**ALTO**
		P R O B A B I L I D A D		

En la siguiente tabla se describe los procedimientos de las medidas preventivas tomadas en detalle, cuando los problemas ocurren.

Las medidas preventivas se dan si, se ha probado, investigado y listado los recursos necesarios para llevarlos a cabo o ejecutarlos, tales como:

- El equipo
- Manual de fallas.
- Funcionamiento de equipos.

Tabla 4.12: Detalles de medidas preventivas del área analizada.

PROCESOS	PROCEDIMIENTO	MEDIDAS ALTERNATIVAS
Proceso de los programas que realizan la entrada y salida de la información	Ingreso y recepción de expedientes (cartas, oficios, informes, etc.) Envío de los documentos a todas las áreas de la institución Salida de documentos (cartas, oficios, informes, etc.)	Puesta en funcionamiento del grupo de Operaciones, Manuales, Puesta en marcha de una red LAN interna.
Mantenimiento adecuado de las aplicaciones	Programación de cronograma de mantenimiento. Elaboración de órdenes de compra y órdenes de servicios	Puesta en funcionamiento del grupo de trabajo. Comunicación con teléfonos móviles.
Equipamiento necesario para un funcionamiento optimo del sistema	Actividades de soporte técnico para casos de fallas Almacén de control de bienes Programación de requerimientos.	Puesta en funcionamiento del grupo de comunicación con teléfonos móviles. Puesta en marcha de una red LAN interna.

4.5. FORMACIÓN Y FUNCIONES DE LOS GRUPOS DE TRABAJO

Se debe determinar claramente los pasos para establecer los grupos de trabajo, desde las acciones en la fase inicial, las cuales son importantes para el manejo de la crisis de administración.

Los grupos de trabajo permanecerán en operación cuando los problemas ocurran, para tratar de solucionarlos.

Tabla 4.13: Funciones de los grupos de trabajo de administración.

DIRECCIÓN ÁREA DE ADMINISTRACIÓN	CARGO DIRECTOR TÉCNICO	FUNCIONES DIRECCIÓN DE ADMINISTRACIÓN
	Especialista	Encargado de la oficina de abastecimientos.
	Especialista	Encargado de la oficina ejecutiva de personal
Área de Software (software interno)	Director Técnico	Dirección técnica de administración de seguridad
	Especialista	Responsable del respaldo de la información Bases de Datos y Aplicaciones
	Especialista	Responsable de configuración e instalación de los programas o aplicaciones
	Director Técnico	Dirección técnica de soporte técnico
	Técnico	Responsable de las PCs y Servidores
Técnica de Soporte	Técnico	Responsable del Software Base
	Especialista	Responsable de Correo Electrónico
	Técnico	Soporte Técnico a usuarios

4.6 DESARROLLO DE LOS PLANES DE ACCIÓN

Se estableció los días en los cuales los problemas son más probables a ocurrir, incluyendo los sistemas del Conjunto de Bodegas, clientes, proveedores e infraestructura de la organización. Se señala los días anunciados, cuando los problemas pueden ocurrir y otros temas.

El siguiente es un cuadro modelo donde debemos señalar exactamente las ocurrencias de fallas y las acciones respectivas aplicadas para cada uno de nuestras realidades.

Tabla 4.14: Lista de acciones ante fallas de recursos.

RECURSO	ACCIÓN	COMO CONFIRMAR	OPERADOR	PROGRAMA PARA LA ACCIÓN	OCURRENCIA DEL PROBLEMA
PC´s	Confirmar la ocurrencia de los problemas	administración comunicara al responsable sobre problemas	Área de Administración	En la mañana	Falla de los PC´s
Software de administración	Confirmar la ocurrencia de los problemas	El administrador de Red supervisará la red e informará problemas	Dirección Técnica de Soporte Técnico	En todo el día	Caída de la red en ciertas áreas
Servidores de Gestión	Confirmar la ocurrencia de los problemas	Administrador de red supervisará e informará problemas	Dirección Técnica de Soporte técnico	En todo el día	Caída de la red en el área de gestión
Sistemas de Gestión	Confirmar la ocurrencia de los problemas	El administrador de los servidores supervisará informará problemas	Dirección Técnica de Soporte	En todo el día	Paralización o fallas en los programas o aplicaciones
Software cliente	Confirmar la ocurrencia de los problemas	Cobertura de los medios	Área de Soporte Técnico	En el día	Caída del sistema en el área de interés.

4.7. ELABORACIÓN DE LISTAS DE PERSONAS Y ORGANIZACIONES PARA COMUNICARSE EN CASO DE EMERGENCIA

Se creará un directorio telefónico del personal considerado esencial para la organización en esas fechas críticas, incluyendo el personal encargado de realizar medidas preventivas y los responsables para las acciones de la recuperación y preparación de medios alternativos.

Este directorio se usa para realizar comunicaciones rápidas con los proveedores de servicio del recurso, incluso con los fabricantes, vendedores o abastecedores de servicio contraídos, si ocurren los problemas, para hacer que investiguen y que identifiquen las causas de los problemas y que comiencen la recuperación de los sistemas

Tabla 4.15: Formato de lista telefónica del personal en caso de una contingencia.

FUNCIÓN	NOMBRE EMPLEADO	PRIMER NUMERO DE CONTACTO	SEGUNDO NUMERO DE CONTACTO	TIEMPO
DIRECCIÓN CARGO				

Tabla 4.16: Formato de lista telefónica de proveedores.

RECURSO	PROVEEDOR DEL SERVICIO	DPTO. A CARGO	SECCIÓN O PERSONA A CARGO	NÚMERO TELEFÓNO

4.8 PRUEBAS Y MONITOREO

En esta etapa hay que desarrollar la estrategia seleccionada, implantándose con todas las acciones previstas, sus procedimientos y generando una documentación del plan.

Hay que tener en claro como pasamos de una situación normal a una alternativa, y de que forma retornamos a la situación normal. Hay situaciones en que debemos de contemplar la reconstrucción de un proceso determinado, ejemplo: por alguna circunstancia dada se determino que la facturación se realice en forma manual, restablecido el servicio que nos llevo a esta contingencia debemos tener el plan como recuperar estos datos para completar la información que día a día utilizan las demás áreas.

Antes de realizar las pruebas, los planes deberían ser revisados y juzgados independientemente en lo que respecta a su eficacia y razonabilidad.

Las pruebas recomendadas para los planes de recuperación de desastres incluyen una prueba periódica preliminar y un ensayo general, en el que se crea un simulacro de una crisis con el fin de observar la eficacia del plan. Las actividades importantes a realizar son:

- La validación de las estrategias de continuidad de los negocios de una unidad de negocios.
- La validación en implementación de un plan (con las operaciones de la empresa y los

representantes de dichas operaciones)

- Realización de pruebas en cada unidad para ver la eficacia de la solución.
- La preparación y ejecución de pruebas integradas para verificar la eficacia de la solución.

La preparación y ejecución de pruebas casos/eventos, probar las respuestas en caso de situaciones de crisis, en base a un caso en el que los eventos ocurren al azar y se intensifican en forma gradual.

CAPITULO V

PRUEBAS DEL PLAN DE CONTINGENCIA

5.1 INTRODUCCIÓN

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la empresa. Las pruebas se efectúan simultáneamente a través de múltiples departamentos, incluyendo entidades comerciales externas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfección en los planes preestablecidos.

5.2 OBJETIVOS

1. Determinar si los planes de contingencia individuales son capaces de proporcionar el nivel de apoyo deseado a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el Plan de Contingencias.
2. Determinar si las pruebas permiten efectuar una valoración detallada de los costos de operación en el momento de ocurrencia de una contingencia.

5.3 NIVELES DE PRUEBAS PARA UN PLAN DE CONTINGENCIA

Se recomiendan tres niveles de prueba:

1. Pruebas en pequeñas unidades funcionales o divisiones.
2. Pruebas en unidades departamentales
3. Pruebas interdepartamentales o con otras bodegas

La premisa es comenzar la prueba en las unidades funcionales más pequeñas, extendiendo el alcance a las unidades departamentales más grandes, para finalmente realizar las pruebas entre unidades interdepartamentales o con otras instituciones externas.

5.4 MÉTODOS PARA PRUEBAS EN LOS PLANES DE CONTINGENCIA

Al desarrollar un plan de contingencia es imprescindible y necesario el desarrollo de pruebas que garantizaran el real desempeño del proyecto, de esta manera existirá mayor credibilidad en el proyecto. A continuación se presenta tres tipos.

5.4.a) Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencias. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

5.4.b) Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Características:

- La discusión se basa en un formato preestablecido.
- Esta dirigido al equipo de recuperación de contingencias.
- Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad

Los ejercicios de escritorio, son ejecutados por el encargado de la prueba y el personal responsable de poner el Plan de Contingencia en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no

cumple con los objetivos propuestos.

5.4.c) Simulación en Tiempo Real

Las pruebas de simulación real, en un departamento, una división, o una unidad funcional de la empresa están dirigidas a una situación de contingencia por un período de tiempo definido.

- Las pruebas se hacen en tiempo real
- Es usado para probar partes específicas del plan
- Permite probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

5.5 PREPARACIONES PRE PRUEBA

- Repasar los planes de contingencia seleccionados para probar.
- Verificar si se han asignado las respectivas responsabilidades.
- Verificar que el plan este aprobado por la alta dirección de la institución.
- Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y la hora para la ejecución de la prueba.
- Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
- No hacer «autoevaluación» la meta es aprender y descubrir las vulnerabilidades, no

generar fracaso y frustración.

- La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.
- Enfocar los procesos comerciales críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.
- Definir el ambiente donde se realizaran las reuniones del equipo de recuperación de contingencias.
- Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

5.6 COMPROBACIÓN DEL PLAN DE CONTINGENCIAS

La prueba final debe ser una prueba integrada que involucre secciones múltiples e instituciones externas. La capacidad funcional del plan de contingencia radica en el hecho, de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

5.7 ENTORNO DE LAS PRUEBAS DEL PLAN DE CONTINGENCIAS

La siguiente tabla de entorno se sugiere para la documentación del Plan de Pruebas:

Tabla No. 5.1 Documentación del plan de pruebas.

1.	*Pruebas de alcances y objetivos*	*El estado que se piensa lograr tras la realización de las pruebas.*
2.	*Pruebas metodológicas*	*Proporciona una descripción del tipo de prueba que se realizará.*
3.	*Precisar equipos y recursos*	*Identifica y establece lo necesario.*
4.	*Demanda de personal capacitado*	*Enumera y describe el personal y las necesidades de capacitación.*
5.	*Detallar itinerarios y localizaciones*	*Desarrolla las tareas, límites, y las responsabilidades que muestran el plan para la ejecución de la prueba.*
6.	*Control del proceso*	*Describe la disposición; desarrollo del escenario de ensayo, y procedimientos*
7.	*Control de la acción del tiempo*	*Detalla la secuencia de eventos para la prueba.*
8.	*Objetivos trazados a partir del control*	*Define las medidas de éxito para la prueba.*
9.	*Control de personal*	*Define los procedimientos para terminar, suspender, y reiniciar la prueba..*
10.	*Pruebas de evaluación y observaciones*	*Detalla los resultados de la evaluación y de la observación, además planes de acción alternados para rectificar fallas.*

5.8 RESUMEN DE LA PRUEBA DEL REPORTE DE ESCRITORIO

5.8.a) Obligación de Mitigar los Daños

Es importante recordar que si los sistemas de Información de PARKENOR fallan y esto da como resultado pérdidas o daños, entonces la compañía tiene una obligación de evitar la acumulación innecesaria de daños adoptando las medidas necesarias para mitigar dichos daños. De igual manera, si ocurren pérdidas a raíz de las acciones de terceros, es posible que la compañía no recupere los daños que a sabiendas permitió que aumentaran. En otras palabras, PARKENOR no debe confiar porque inicialmente no fue su culpa y simplemente suponer que la parte culpable se responsabilizará de todas las pérdidas y daños resultantes. PARKENOR debe adoptar algún tipo de acción para minimizar el impacto sobre sus negocios, y los daños a la propiedad, resultantes de una falla del sistema de información.

En la práctica, un plan de contingencia puede y debe ser visto como una herramienta para cumplir con esta obligación legal: el plan resumirá los pasos que la compañía dará para mitigar sus daños en caso de que ocurra una falla. Por supuesto que la falta de un plan no eliminará la obligación de mitigar, y el hecho de que no haya un plan podría ser empleado en contra de PARKENOR en un litigio subsecuente como evidencia de que no adoptó las medidas suficientes para minimizar el daño incurrido. Los peritos podrían atestiguar que el plan de contingencia para el sistema de información era necesario, y que la ausencia de un plan era irrazonable y que el acusado no debería sufrir las consecuencias.

Para complicar aún más las cosas, un plan de contingencia debería tomar en cuenta

también cualquier otro sistema para la determinación de prioridades que pudiera haber sido utilizado por una compañía, u otros procesos utilizados para enfocar los sistemas que tienen una importancia crítica para la misión. El "sistema para determinar prioridades" se refiere a la práctica utilizada durante la guerra de separar a los soldados heridos en categorías, poniendo a un lado a los que probablemente sobrevivirían aún sin atención médica, aquellos que probablemente morirían sin importar lo que se hiciera por ellos, y aquellos para los cuales la atención médica era de importancia crítica; la atención médica se centraba en las personas que se encontraban en esta última categoría.

Dos lecciones claves surgen. Primero, es importante evaluar los impactos económicos de los sistemas de computación, y utilizar el plan de contingencia como un vehículo para mitigar las pérdidas económicas tanto para el negocio como por razones legales. Segundo, el plan de contingencia debería enfocar no solamente los sistemas considerados críticos para la misión. Debería enfocar todos los sistemas, y hasta cierto grado el plan de contingencia puede ser aún más importante desde el punto de vista legal para las aplicaciones no críticas que se espera que fallen.

5.8.b) Meta: Documentación de un Plan

Por supuesto que un plan de contingencia tiene un valor limitado desde el punto de vista comercial o legal, si no fue redactado por escrito y si no se mantiene adecuadamente en lugares de fácil acceso para el personal clave. Generalmente, para propósitos legales, para evitar y defender cualquier alegato de negligencia o falta de cuidado debido a la inoperancia. Es de importancia crítica que los planes de contingencia sean revisados apropiadamente para que se acoplen al sistema de

información, con los jefes de equipo y los funcionarios y/o los miembros de las juntas directivas y además que dichas acciones sean tomadas con una anticipación suficiente ante cualquier problema, con el fin de permitir el tiempo suficiente para los comentarios, reacciones e implementación de las mismas, ya que un plan de contingencia requiere de negociación y seguimiento. Además, si se decide que no se necesita ningún plan de contingencia, esa decisión debería estar adecuadamente documentada y explicada a la luz de la atención que se está dando actualmente a los planes de contingencia. En última instancia, la compañía querrá evitar cualquier responsabilidad individual de sus directores y funcionarios bajo el reglamento del "juicio de la empresa", aseverando que todas sus decisiones en cuanto a la forma de manejar las contingencias del Sistema de Información fueron debidamente consideradas, y/o que se basó en las opiniones de los expertos en los que la compañía razonablemente confió para formular un plan de contingencia.

Después de la documentación del Plan de Contingencia y su aprobación por el comité técnico a cargo de dicho plan, las copias se distribuyen a todas las áreas de la organización.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES.

- El desarrollo de un plan de contingencia permite disminuir el impacto y los efectos de una catástrofe.
- Usar un lenguaje común sobre desastres con el personal permite efectuar acciones eficientes en caso de calamidades.
- La capacitación del personal permite evitar desastres y en caso de haberlos minimizar perdidas.
- La actualización en la información del personal permite desarrollar eficientemente acciones de emergencia en caso de accidentes.
- La identificación de áreas vulnerables críticas permite tomar acciones preventivas y evitar accidentes.
- La creación de un equipo de emergencia permanente permitió dar mayor seguridad al Conjunto de Bodegas PARKENOR

6.2 RECOMENDACIONES

- Realizar prácticas y evaluaciones del Plan de Contingencia 2 veces por año.
- Permitir que este trabajo sea aplicado periódicamente en PARKENOR.
- Actualizar la información del personal de manera oportuna.
- Elaborar un mapa de riesgo con la información obtenida de las distintas fuentes; acciones de las distintas bodegas y la metodología de aplicación, con el fin de identificar zonas vulnerables donde se deba realizar una labor preventiva más intensa.
- Elaborar y difundir campañas informativas y de sensibilización dirigidas al personal, orientadas a concienciar sus deberes con PARKENOR..
- Dotar de equipos de protección eficientes, sistemas de vigilancia activa y pasiva frente a los riesgos, para prevenir y proteger PARKENOR.
- Mantener Vías de Evacuación suficientes y libres de obstrucciones.
- Disponer señalización necesaria para las Vías de Evacuación y equipos contra incendio.
- Disponer equipos de combate de incendios y personal capacitado en su uso.
- Contar con una Organización de Emergencia de carácter permanente.
- Difundir y coordinar entre todo el personal y empresas ajenas (mantenimiento, proveedores, clientes etc.) el plan de contingencia de PARKENOR
- Crear mecanismos de coordinación y colaboración con ayudas exteriores (Bomberos, Policía, Defensa Civil.) ante su posible intervención en caso de emergencias.
- Elaborar y cumplir procedimientos y manuales sobre normas de Seguridad del Personal de PARKENOR. (Manual de Seguridad y prevención de riesgos).

ANEXO **A**

PLAN PARA LA CONTINUIDAD DE NEGOCIOS

Nombre de la compañía: Conjunto de Bodegas PARKENOR
Dirección: AV. 10 DE AGOSTO KM 5.5

Ciudad: QUITO

Número telefónico: 02 2484 004

Conjunto de Bodegas PARKENOR

La siguiente persona estará a cargo de gestionar la crisis y será la portavoz de la compañía en caso de emergencia

Sr. Fabián Ruiz
Contacto primario de emergencia

096851840
Número de teléfono

022484004
Numero alternativo

Fabianruiz@hotmail.com
Correo electrónico

Si la persona no puede gestionar la crisis, esta otra persona será quien esté a cargo

Sra. Marcia Morales
Contacto secundario de emergencia

022484004
Número telefónico

022686604
Numero alternativo

Mmorales@hotmail.com
Correo electrónico

INFORMACIÓN DE CONTACTOS DE EMERGENCIA

CRUZ ROJA 131

Emergencia

POLICIA 101 – BOMBEROS 102

Policía - Bomberos (no emergencia)

SEGUROS EQUINOCCIAL 2445602

Proveedor de seguros

PC PLUS 096 851 840

Proveedor informático

1. MANTENGASE INFORMADO SOBRE DESASTRES

Cuáles son los desastres naturales y causados por el hombre que podrían afectar nuestro negocio.

Terremoto
Incendio
Inundación y humedad
Corte de Energía
Falla de la red de voz y datos
Fallas en Hardware o Software
Sabotaje o daño accidental
Vandalismo y manifestaciones

2. EQUIPO DE PLANIFICACIÓN DE EMERGENCIA

Las siguientes personas intervendrán en la planificación de emergencias y la gestión de crisis de manera directa y serán las primeras en tomar decisiones sobre la crisis.

ROLES	PUESTO	OCUPANTE ACTUAL
Presidente del Grupo de Trabajo	Presidente de PARKENOR	PRESIDENTE PAKENOR
Coordinador General	ADMINISTRACIÓN DEPARKENOR	Sr. Fabián Ruiz F.
Coordinador	Secretaría de la ADMINISTRACIÓN	Sra. Marcia Morales
Coordinador de Redes	Administrador de Redes y Comunicaciones	Sr. Romel Lara S.
Coordinador Soporte Técnico	Mantenimiento y Soporte Técnico	Sr. Romel Lara S.

3. EQUIPO DE PLANIFICACIÓN EXTERNA

Las siguientes personas de las empresas que conforman el Conjunto de Bodegas PARKENOR participaran del equipo alterno de emergencias.

NOMBRE propietario	DIRECCIÓN	TELEFONO
Isabel Bonilla	**Juan Barrezueta N70-71 y Moisés Luna**	2479-936 2479-621
COMANDATO	**Av. 10 de Agosto y Naciones**	
Susana Morales	**Juan Barrezueta N70-71 y Moisés Luna**	2267-451 2452-453
Marco Molina	**Av. De los Shyris 2317 entre el telégrafo y el Universo junto al restaurante Jardín de China**	2252-725 099445616
Javier Sarango	**Av. De los Shyris y República del Salvador 2do piso**	2262-728 ext. 2072
Edgar Aldas	**Wandemberg E6-160 y Botadano**	2810-165 2409-443
Eugenia Camacho	**Calle san José y segunda trasversal**	3260213 096010308
Sr. Fabián Castro	**Manuel Larrea 311 y Arenas Sector Consejo Provincial**	2564-550
Tcrnl. Agustín Yépez	**Gonzalo Gallo OE-91 308 y Manuel Serrano**	2240-536
Roberto Juriss	**Gonzalo Gallo OE4-91y Manuel Serrano**	2435-529 098939170
Sonia Valencia	**Murgón 384 y Ulloa**	2524-666
Víctor Hugo Jiménez	**Ulloa 650 y Marchena**	2230-199
Carlos Torres	**Naciones Unidas y Amazonas Edf. Unicornio piso 11**	2463-623 2467-616
Texaco Petroleum Company (Arrendatario)	**Rumipamba E2-209 y Av. República Edificio Borja Páez 1 Piso Ofic. 12**	Sr. Diego Borja 2262-709 / 2921-810 097695349
Francisco Calisto (Pablo Hidalgo)	**Reina Victoria N25-33 y Av, Colón Edfi. Banco de Guayaquil 4to piso Of. 405-A-B**	2504-477 2569-832 099691204
Gilberto Tenesaca		2390-322 2391-851
Mundy Home	**Tomas de Berlanga E4-85 Y Amazonas (frente a la plaza de toros)**	2258-798 2258-799

Justo Prieto (Genaro Cruz)	**Av. Marchena OE-256 y Versalles Edf. Ladrillo 1er piso Ofic. 1**	2505-966 2224-534 / 098534330
IMPORTVAC **Sr. Cristian Vaca**	**Gregorio Bobadilla N36-24 y NNUU**	2277-105 Celu. 096527063
Mecadec (Arrendatario)	**Av. Amazonas 4080 y Naciones Unidas Edif. Puerta del Sol Torre "Este" Oficina 406**	Srta. Sara Arias 2261-767 2261-768
Leonor Álvarez	**Gonzales Suárez 869 Edfi. Casa Bella**	2362-036 2363-732
Eduardo Cordero	**Mariano Echeverría OE-443 y Brasil**	2483-735 099738180
BANRED (Arrendatario)	**Av. 9 de Octubre N19-33 Edificio ETECO Piso 6 (El Ejido, frente al Banco Internacional)**	Stra. Karina Tamayo 2502-018 fax 2238-884
Byron Checa	**Pasaje Yaupi y Mariana de Jesús**	2562-123 2562-124
Jorge Estrella	**Julián Arbaiza E7-69 y Pedro Cornelio**	2411-724 2813-131 2404-789
Jorge Robalino/Sra. Emma Andrade	**Calle Boyacá 161 y Av. Universitaria Sector Miraflores Casa 19-61**	fax 2567610 098301088
Jorge del Salto	**Las Avellanas N67-4**	2801-123 2801-124 099708038
Patricio Vascones	**Guayaquil**	042434354
Nicolás Gallardo	**Wimper y Orellana**	2905-290 2905-289 2223-554
Sr. Víctor Chiriboga	**Av. 6 de diciembre 2816 y Paul Rivet**	2222-600 2222-601
Cyede	**Luis Cordero e Isabel la Católica esquina**	2231-322 ext.121 2507-961
Byron Amores	**Av. 6 de Diciembre 5247 y el Telégrafo Edf. García Ayala No.- 2**	
Hernán López	**Japón y Pereira Lote No.- 3**	2267-268 2270-271
Guillermo Herrera	**Mariano Aguilera E7-36 y la Pradera**	2506-349 2506-353 099721523
Fabián Echeverría	**Av. República y la Pradera**	2227-700 ext. 2110
Juan Serrano (Liquidador)	**Av. 6 de Diciembre y Colón Edf. Parkienon 9no piso Ofic. Cife**	2200-277 099257528

4. PROVEEDORES Y CONTRATISTAS

Son las empresas donde obtenemos suministros/materiales:

Nombre de la compañía: Punto net

Dirección: Amazonas 45-45 y Pereira

Ciudad: Quito

Teléfono: 298 9900

Correo electrónico: www.puntonet.ec

Nombre del contacto: Punto net

Materiales/Servicios prestados: Servicios de Internet

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: ANDINANET

Dirección: Veintimilla y Amazonas

Ciudad: QUITO

Teléfono: 1800 378 466

Materiales/Servicios prestados: Servicios de internet

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: INTERACTIVE

Dirección: **www.interactive.com**

Ciudad: QUITO

Teléfono: 298 6440

Materiales/Servicios prestados: Servicios de Internet.

Nombre de la compañía: SUMINISTROS DE COMPUTACIÓN

Dirección: Legarda Oe7 y Pedro de Alvarado

Ciudad: QUITO

Teléfono: 265 1937

Correo electrónico: www.compucintas.com

Nombre del contacto: COMPUCINTAS

Materiales/Servicios prestados: Suministros de computación

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: Suministros y Suministros

Dirección: Francisco Salazar e10-22 y Tamayo

Ciudad: QUITO

Teléfono: 8003350

Materiales/Servicios prestados: Suministros de computación

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: COMPU LAB

Dirección: 9 de octubre N22-59

Ciudad: QUITO

Teléfono: 2228584

Materiales/Servicios prestados: Suministros de computación

Nombre de la compañía: PC Plus

Dirección: Cardenal de la Torre y Ajaví

Ciudad: QUITO

Teléfono: 096851840

Correo electrónico: lararomel@hotmail.com

Nombre del contacto: Romel Lara

Materiales/Servicios prestados: Mantenimiento preventivo de computadores

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: Digital Mate

Dirección: Edmundo Carvajal Oe5-295 y Ramiro Barba

Ciudad: QUITO

Teléfono: 2432989

Materiales/Servicios prestados: Mantenimiento preventivo de computadores

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: INACORP

Dirección: Juan Severino E6-80 y Eloy Alfaro

Ciudad: QUITO

Teléfono: 2904120

Materiales/Servicios prestados: Mantenimiento preventivo de computadores

Nombre de la compañía: Seguros Colonial

Dirección: Av. Amazonas N44-105 y Rio Coca

Ciudad: QUITO

Teléfono: 1800 222 000

Correo electrónico: www.seguroscolonial.com

Nombre del contacto: Seguros colonial

Materiales/Servicios prestados: Servicio de seguros informáticos

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: INTEROCEANICA

Dirección: Av. amazonas N35-17 y Juan P. Sanz

Ciudad: QUITO

Teléfono: 1800 SEGUROS

Materiales/Servicios prestados: Servicio de seguros informáticos

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: LA UNION

Dirección: Av. 6 de Diciembre 25-20 y Orellana

Ciudad: QUITO

Teléfono: 222 0648

Materiales/Servicios prestados: Servicio de seguros informáticos

Nombre de la compañía: INSOFT

Dirección: General Roca N32-262

Ciudad: QUITO

Teléfono:

Correo electrónico: www.e-insoft.com

Nombre del contacto: INSOFT

Materiales/Servicios prestados: SOFTWARE ADMINISTRATIVO

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: INGELSI

Dirección: www.ingelsi.com

Ciudad: QUITO

Teléfono: 248 48838

Materiales/Servicios prestados: SOFTWARE ADMINISTRATIVO

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: SATCOM

Dirección: VENTAS@SATCOMEC.COM

Ciudad: QUITO

Teléfono: 2559275

Materiales/Servicios prestados: SOFTWARE ADMINISTRATIVO

Nombre de la compañía: PC PLUS

Dirección: Cardenal de la Torre y Ajaví

Ciudad: QUITO

Teléfono: 096851840

Correo electrónico: lararomel@hotmail.com

Nombre del contacto: Romel Lara S.

Materiales/Servicios prestados: VIGILANCIA DIGITAL

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: DELTA SYSTEMS

Dirección: Mañosca N36-09

Ciudad: QUITO

Teléfono: 2250551

Materiales/Servicios prestados: VIGILANCIA DIGITAL

Si esta compañía sufre un desastre, obtendremos suministros/materiales de la siguiente:

Nombre de la compañía: CARRERA ESTRADA Y ASOCIADOS

Dirección: WWW.BROWSE.CL

Ciudad: QUITO

Teléfono: 2441911

Materiales/Servicios prestados: VIGILANCIA DIGITAL

5. PLAN DE EVACUACIÓN PARALAS INSTALACIONES

- ✓ Hemos elaborados los planes de evacuación con la colaboración de los copropietarios de del Conjunto de Bodegas PARKENOR para evitar confusiones y embotellamientos.
- ✓ Hemos desarrollado, copiado, y publicado mapas del edificio y de las instalaciones.
- ✓ Las salidas están claramente marcadas.
- ✓ Se practicará procesos de evacuación **2 veces** por año.

Si debemos refugiarnos rápidamente, en caso de inundaciones, sismos, incendios, vandalismo.

Sistema de advertencia

Probaremos el sistema de advertencia y registraremos los resultados **3 veces** por año.

Lugar de reunión: **GARITA DE PARKENOR**

Gerente y auxiliar a punto de evacuación: **Sr. FABIAN RUIZ, Sra. MARCIA MORALES**

Algunas responsabilidades: asignación de labores, asignación de responsabilidades, coordinación del personal, coordinación de evacuaciones.

Sr. FABIAN RUIZ, es el único responsables de declarar **Todo controlado.**

6. PLAN DE REFUGIOS: GARITA PARKENOR

El personal de PARKENOR se encuentra al tanto sobre los suministros de emergencia, si existen, están en buenas condiciones, son de libre acceso, los proporciona la empresa en el lugar del refugio, y cuáles son los suministros de emergencia que se pueden considerar guardar en un kit portátil.

Se practicará los procedimientos de refugio **2 veces** por año

SI DEBEMOS REFUJIAR LOS EQUIPOS RAPIDAMENTE

Utilizar la garita, el primer y segundo piso en caso de emergencia.

Sistema de advertencia: El administrador o auxiliar es el único encargado de dar la vos de alarma.

Probaremos el sistema de advertencia y registraremos los resultados **2 veces** por año

Lugar de refugio tormentas: segundo piso garita PARKENOR

Lugar de refugio terremotos: primer piso garita PARKENOR

Lugar de refugio incendios: primer piso garita PARKENOR

Lugar de refugio inundaciones: segundo piso garita PARKENOR

Lugar de refugio vandalismo: segundo piso garita PARKENOR

Administrador del refugio y ayudante: Sr. Fabián Ruiz, Marcia Morales

Algunas actividades: coordinar acciones para restablecer actividades que permitan reanudar parcial o totalmente las labores de PARKENOR.

Personal alternativo responsable: Marcia Morales, Jefe de personal

En caso que el administrador o ayudante no puedan acudir inmediatamente serán responsables de tomar decisiones de acuerdo a comunicación establecida con el administrador general.

El Administrador bajo el control del PRESIDENTE de PARKENOR es el responsable de emitir la señal de ***TODO DESPEJADO.***

7. COMUNICACIONES

Comunicaremos nuestros planes de emergencia con compañeros de trabajo de la siguiente manera:

Vía reuniones.

Por medio de órdenes verbales

Por medio de simulacros

En caso de un desastre, nos comunicaremos con los empleados de la siguiente forma.

Vía teléfono celular

Vía telefonía convencional

Vía Motorola

8. SEGURIDAD INFORMATICA

Para proteger nuestro hardware haremos lo siguiente:

Revisión de garantías en os equipos

Control del área eléctrica

Usar áreas de trabajo viables.

Para proteger nuestro software haremos lo siguiente:

Definir los procedimientos que indiquen los datos, programas, etc., que es importante respaldar; por servidor, sistema y ubicación.

Identificar cada uno de los métodos que se utilizan, para llevar a cabo los respaldos de información, así como los procedimientos para su ejecución y restauración.

Especificar el lugar donde se encuentran custodiados los respaldos de información o copia de los respaldos, ya sea en un lugar fuera de las instalaciones o en una Institución Bancaria.

Si las computadoras resultan destruidas, utilizaremos computadoras de seguridad en el siguiente lugar: **Segundo piso de la garita de PARKENOR.**

COPIA DE SEGURIDAD DE LOS ARCHIVOS.

Sr. Fabián Ruiz es el responsable de realizar las copias de seguridad de nuestros archivos importantes, incluido nomina, contabilidad, seguridad.

Las copias de seguridad, incluyendo una copia de este plan, mapas del sitio, seguros, copias de seguridad informática se encuentran en **ARCHIVO controlado por la SRA. MARCIA MORALES** y **Sr. FABIAN RUIZ F.**

Otro juego de copias de seguridad se encuentra fuera de las instalaciones, **en manos del presidente de PARKENOR.**

Si los registros de contabilidad y nomina de personal resultan destruidos, mantendremos la continuidad de la siguiente forma: **existe un servidor informático donde se encuentra toda la información. Las actualizaciones de la información están en copia de seguridad.**

9. INFORMACIÓN DE CONTACTO DE EMERGENCIA DE LOS EMPLEADOS

PUESTO	NOMBRE	TELEFONO
Presidente PARKENOR	Presidente de PARKENOR	
Administrador General	Fabián Ruiz F.	098903103
Secretaria general	Sra. Marcia Morales	022484004
Mantenimiento-seguridad	Sr. Romel Lara	092531511

REVISION ANUAL

Revisar y actualizar este plan de continuidad de negocios y desastres en **12 meses.**

Bibliografía

[1] Ministerio Coordinador de la Seguridad Interna y Externa, Secretaria Técnica de Gestión de Riesgos, Defensa Civil del Ecuador., "Plan de Continuidad de Actividades Ante Emergencias", Departamento de Capacitación Quito-Ecuador 2009

[2] Ministerio Coordinador de la Seguridad Interna y Externa, Secretaria Técnica de Gestión de Riesgos, Defensa Civil del Ecuador., "Propuesta de Estrategia Nacional para la Reducción de Riesgos y Desastres", COEM, Departamento de Capacitación Quito-Ecuador Noviembre 2008

[3] José de Jesús Félix Hernández. "Guía Práctica para el Desarrollo de Planes de Contingencia". Lima, febrero 2008.

[4] INEI "Seguridad de la Información", Elaboración Sub-jefatura de informática. Versión 1.0 - 10/01/2009.

[5] CONIDA "Plan de Contingencia de Equipos Informáticos", Comisión de investigación y Desarrollo Aeroespacial. Directiva 13/2007 CONIDA/OGA.

[6] Por qué se necesita un **Plan de Contingencia?**
www.monografias.com/trabajos11/.../plconting.shtml -

[8] Gina Lizbeth Maza "Plan de Contingencia Informático y Seguridad de Información 2009, Aplicado en la Universidad Nacional de Piura", 2007.

Dedicatoria

Con todo el cariño del mundo dedico este trabajo a mi querido hermano Walter, quien siempre está a mi lado y lo recuerdo mucho.

Romel

Agradecimiento

Al ser Supremo, quien tiene los caminos más raros para hacernos entender que no estamos solos.

De manera muy especial a mis hermanas Iralda y Silvia, ellas fueron determinantes para la consecución de este proyecto.

Agradecimiento

De manera muy especial al Ing. Mario Ron, Ing. Carlos Caizaguano, Ing. Danilo Martínez.

A todos, mil gracias.

Contenido

Índice de Tablas.

CAPITULO I

CAPITULO III

CAPITULO IV

CAPITULO V

Índice de Figuras

Índice de Anexos

.

RESUMEN

Un plan de contingencia implica el análisis de posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, es así que su objetivo es reducir el riesgo sobre la posibilidad de ocurrencia de siniestros en el área de hardware, software, información y equipos periféricos. Además este documento tiene como objetivo establecer procedimientos que permitan reducir el riesgo de siniestro de cualquier índole, teniendo como alcance a todo el personal de PARKENOR sea cual fuere su régimen laboral. La elaboración de equipos de emergencia permitió asignar grados de responsabilidad, desarrollar un Plan de Continuidad de Negocios, adquirir seguros, desarrollar un análisis de riesgos, y la implementación de soluciones, permitiendo que el Conjunto de Bodegas. PARKENOR posea un Plan de Contingencias Informático. Los resultados en simulacros de emergencia prueban que el personal sin reglamentos y capacitación en el área de desastres poco a nada puede hacer y las pérdidas materiales y personales pueden ser incalculables, por este motivo es necesario el entrenamiento del personal, la difusión del documento desarrollado y la actualización periódica de la información.

ABSTRACT

A contingency plan involves analysis of potential risks which may be exposed to computer equipment and the information contained in various storage media, so that its objective is to reduce risk on the possibility of occurrence of accidents in the area hardware, software, and peripherals. Furthermore, this document aims to establish procedures to reduce the risk of loss of any kind, with the scope to all staff irrespective PARKENOR labour regime. The development of emergency teams allowed assigning degrees of responsibility, developing a Business Continuity Plan, purchasing insurance, developing a risk analysis, and implementation of solutions, allowing the Joint Wineries. PARKENOR holds a Computer Contingency Plan. The results show that emergency drills without regulations and staff training in the disaster area can do little to nothing and personal and material losses can be incalculable, for this reason it is necessary to train staff dissemination of the document developed and regular updating of information.