CAPITULO I

INTRODUCCIÓN

Los desastres informáticos pueden presentarse en cualquier lugar y momento; ya sean estos de forma inducida o por desastres naturales y nadie está libre de estos, es por eso que toda empresa sin excluir a ninguna debe contar con un plan de contingencias contra desastres informáticos.

En el momento se ha vuelto un problema los ataques cibernéticos con el avance vertiginoso de la tecnología cada día es más complicado contrarrestar a los hackers, y no solo eso existen desastres naturales que podría paralizar cualquier ámbito comercial, es por eso que una herramienta muy poderosa que se está implementando en las Empresas es desarrollar un plan de contingencias contra desastres informáticos si es que no lo tiene.

Con los antecedentes que se ha tenido en la Empresa Cartopel S.A.I. he propuesto a la empresa realizar un estudio para la implementación de un plan de contingencias contra desastres informáticos como tesis de graduación, con este estudio la empresa podrá prevenir pérdidas irreversibles sobre todo protegiendo el tesoro más preciado de cualquier empresa que es su información.

1.2. PLANTEAMIENTO DEL PROBLEMA

Falta de un Plan de Contingencia contra desastres informáticos en el área de producción del Grupo Cartopel S.A.I. ubicado en el Parque Industrial de la Ciudad de Cuenca.

1.3. ANTECEDENTES

Hoy en día la informática está enrolada en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar sometidos a las leyes generales de la misma, en consecuencia, las organizaciones informáticas forman parte del denominado “gestión de la empresa”.

Por ende, debido a su importancia en el funcionamiento de una empresa, existen los Planes de Contingencia ya que la información es un recurso que al igual que los otros activos, tienen mucho valor para una Empresa, por lo tanto esta debe ser totalmente protegida.

Cabe indicar que los eventos naturales, son la causa de algunos desastres informáticos, pero aún más el sistema en el cual nos encontramos esto es el medio social, político, y económico (diferente del medio ambiente natural), que estructuran de manera diferente la vida de los distintos grupos de personas.

Por este motivo al analizar la gestión de los desastres, debe darse énfasis tanto a las amenazas naturales propiamente dichas como al ambiente social y sus procesos. Los desastres no deben ser tratados como eventos peculiares que merecen su propio enfoque sectorial, sino como una expresión de la problemática social o como problemas no resueltos del desarrollo, donde la vulnerabilidad no sólo es una característica de diferentes peligros o amenazas sino sobre todo de los procesos económicos, políticos y sociales

Es necesario mencionar que los desastres no se pueden evitar pero si se puede estar listos para cuando lo sucedan gracias a un estudio realizado con anterioridad y con un plan de contingencia en el área de producción ya que la empresa no cuenta con dicho plan en una área tan importante y punto clave para el progreso de la empresa.

1.3.1. Diagnóstico.

La Empresa Cartopel S.A.I. es una empresa de producción al servicio de la ciudadanía por 20 años, luego de análisis exhaustivo se ha detectado la necesidad de disponer de

mecanismos para garantizar la confidencialidad, integridad y disponibilidad de los mismos, dicha entidad ha visto la necesidad de implementar políticas de seguridad informáticas que permitan concienciar a cada uno de los funcionarios de la empresa sobre la importancia y sensibilidad de la información.

Cuenta con políticas creadas, frente a cada una se elaborará un plan de contingencia que permita dar una respuesta oportuna, adecuada y coordinada a una situación de emergencia causada por fenómenos destructivos de origen natural o humano.

Para un correcto uso de las políticas de seguridad y una aplicación correcta del plan de contingencia, analizara y propondrá un nuevo esquema de red que ayude a compartir recursos y a comunicar de mejor manera a cada uno de los miembros que laboran en sus departamentos.

1.3.2. Causas y Efectos

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

1.3.2.1. Incendios

Causa.- Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

Efecto.- El fuego es una de las principales amenazas contra la seguridad de las computadoras, ya que puede destruir fácilmente los archivos de información y programas.

1.3.2.2. Inundaciones

Causa.- Es la invasión de agua por exceso de escurrimientos superficiales es una de las causas de mayores desastres en centros de cómputos.

Efecto- El agua daña los circuitos electrónicos, lo que trae como consecuencia el daño y pérdida de información.

1.3.2.3. Condiciones Climatológicas

Causa.- Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares.

Efecto.- Estos cambios climatológicos ocasiones las variaciones de energía eléctrica, como consecuencia de eso se pueden quemar los CPU.

1.3.2.4. Terremotos

Causa.- Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o muy intensos que trae serios efectos.

Efecto.- Destrucción de edificios con todo su contenido y hasta la pérdida de vidas humanas.

1.3.2.5. Instalaciones Eléctricas

Causa.- Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física.

Efecto.- En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

1.3.2.6. Acciones Hostiles

a.- Robo Informático

Causa.- Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

Efecto.- La información importante o confidencial puede ser fácilmente copiada sin dejar ningún rastro.

b.- Fraude Informático

Causa.- Por esta causa millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Efecto.- debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien que perder en imagen, no se da ninguna publicidad a este tipo de situaciones.

c.- Sabotaje Informático

Causa.- El peligro más temido en los centros de procesamiento de datos, es el sabotaje, los imanes son las herramientas a las que se recurre.

Efecto.- Con una ligera pasada del imán la información desaparece.

1.3.3. Pronóstico

La falta de un Plan de Contingencia contra desastres informáticos dentro del área de producción, ocasionará a corto o mediano plazo la pérdida de recursos económicos, materiales y humanos para la empresa.

1.3.4. Control de Pronóstico

Es necesario proceder con el estudio de un plan de contingencias contra desastres informáticos del área de producción en el grupo Cartopel S.A.I., para asegurar los bienes materiales (hardware y software) y sobre todo la información que es lo más importante y si llega a darse un desastre estar preparados tomando las medidas necesarias solo rigiéndose al plan de contingencias.

1.4. OBJETIVOS

1.4.1. Objetivo General

Análisis de un plan de contingencia contra desastres informáticos en el área de producción del Grupo Cartopel S.A.I.

1.4.2. Objetivos específicos

1. Definir los mayores riesgos que pueden presentarse en la Empresa.
2. Especificar las acciones que se pueden realizar para disminuir estos riesgos.
3. Establecer un procedimiento formal y escrito que indique las acciones a seguir para afrontar con éxito un accidente, incidente o emergencia, de tal manera que los servicios se restablezcan en el menor tiempo posible y con el menor impacto tecnológico.
4. Conocer las ventajas y desventajas de un plan de contingencias.

1.5. JUSTIFICACIÓN

1.5.1. Justificación Teórica

La Empresa Cartopel S.A.I, tiene como objetivo principal la producción se encuentra ubicada en el Parque Industrial, durante los últimos veinte años Cartopel 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 Cartopel necesita realizar un conjunto de procedimientos y reglas a seguir para que en caso de accidentes no afecten de alguna manera los sistemas informáticos del Grupo Industrial.

El Grupo Cartopel al estar constituido por varias empresas, sus asociados han visto en la necesidad de crear acciones positivas 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 Grupo.

El objeto de la investigación descriptiva consiste en evaluar ciertas características de una situación particular en uno o más puntos del tiempo.

En esta investigación se analizan los datos reunidos para descubrir así, cuales variables están relacionadas entre sí.

Se debe llevar a cabo los siguientes pasos:

1. Identificación y delimitación del problema.
2. Formulación de la hipótesis.
3. Procesar los datos, recopilar organizar, clasificar, comparar e interpretar.
4. Extracción de conclusiones.
5. Redacción de informe final.

1.5.2. Justificación Práctica

El Análisis e Investigación dará como resultado un estudio muy importante sobre como tener protegido los recursos informáticos de Cartopel y así de manera segura contar con la confidencialidad de los datos; es decir, tener privacidad de los elementos de información almacenados y procesados en el sistema informático.

También se podrá controlar la integridad de la información y datos esto se refiere a la validez y consistencia de los elementos estos deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Los impactos que se tendrían:

Tecnológico: Se podrá analizar los mejores métodos que se utilizan actualmente para proteger la integridad y confidencialidad de la información y de los datos

Económico: ahorro de dinero ya que con este análisis el gerente de la empresa podrá estar preparado para cualquier problema que exista en la empresa.

Social: ayudara en el medio para que las empresas puedan trabajar de una manera más segura y así no tengan que estar preocupándose o con el temor de que en su empresa pueda haber desastres informáticos.

1.5.3. Justificación Metodológica

En la Empresa Cartopel es necesario realizar una investigación de un plan de contingencias contra desastres informáticos, lo cual implica realizar una serie de actividades las mismas que detallo a continuación:

1.- Establecer los mayores riesgos que pueden presentarse en la Empresa.
2.- Ubicar al personal que está vinculado con las áreas más vulnerables.
3.- Buscar alternativas o mecanismos para prevenir los desastres informáticos.

Estas acciones ayudaran a prevenir algunas perdidas informáticas a consecuencia de los desastres las mismas que pueden ser provocadas por la naturaleza o por el ser humano.

CAPITULO II

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

2.1.1. Introducción al plan

El Plan de Recuperación de Desastres y Continuidad del Negocio (PRD/CN), es un proceso de manejo integrado que identifica el impacto de potenciales amenazas que tiene la empresa Cartopel la misma provee un marco de procesos y procedimientos para construir una respuesta con las capacidades necesarias para que sea efectiva, salvaguardando los intereses de los accionistas y funcionarios, conforme a la naturaleza, escala y complejidad de las actividades de la Institución.

Implica que en cualquier momento en que se identifiquen las amenazas de interrupción, ocasionada por factores externos y sobre los cuales no tiene control la empresa; esta tenga la habilidad de priorizar exitosamente los esfuerzos de varios especialistas de diversas áreas para resguardar efectivamente los intereses de la empresa y superar eficientemente la pérdida de parte o de toda la capacidad operacional instalada.

El Plan de Recuperación de Desastres y Continuidad del Negocio, se realiza en el marco de la metodología - Business Continuity Management – Gestión de la Continuidad del Negocio (GCM) de Janco Associates Inc. Incluye las siguientes etapas:

Grafico No.1: “Ciclo de vida para gestionar la Continuidad del Negocio”

El desarrollo de estas etapas y la aplicación de los conceptos y formatos del método en el contexto del negocio del Cartopel.

En el Plan de Contingencia Informático se establecen procedimientos preventivos para el manejo de casos de emergencia que se presenten en la Empresa Cartopel S.A.I. 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.

2.1.2. Tipos de Contingencias

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 incendio, inundación, terremoto etc.

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.

2.1.3. 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.

2.1.4. Preparación del proceso

El propósito de esta etapa es formalizar el desarrollo del Plan de Recuperación de Desastres y Continuidad del Negocio; por una parte, define la voluntad política de la Institución para desarrollar el plan; por otra, define el objetivo, contexto, estándares y supuestos que se consideran para el desarrollo del plan; y, finalmente se realiza un análisis del contexto del negocio que servirá de marco de referencia para desarrollar una estrategia de contingencia adecuada.

Objetivos específicos de esta etapa:

- Definir políticas y responsabilidades para el desarrollo del plan
- Identificar el objetivo, alcance, restricciones y consideraciones a tener en cuenta
- Analizar el contexto del negocio
- Valorar la criticidad de los procesos de negocio

2.1.5. Autorización

En la empresa Cartopel en concordancia con su estrategia tendiente a satisfacer las necesidades de sus clientes, lo que involucra necesariamente garantizar la continuidad del servicio y recuperarse rápidamente en caso de producirse un desastre no previsto; y por otro lado, consciente de la dependencia operacional de las Tecnologías de Información y de Comunicaciones (TIC), autoriza el estudio, preparación, implementación y mantenimiento de

un Plan de Recuperación de Desastres y Continuidad del Negocio (PRD/CN) para asegurar una respuesta a eventos que podrían atentar a la capacidad operacional de la empresa Cartopel.

2.1.6. Objetivos y Alcances del Plan

El objetivo de contar con un Plan de Recuperación de Desastres y Continuidad del Negocio -PRD/CN- es establecer responsabilidades concretas, acciones y procedimientos para recuperar la capacidad operacional de la empresa Cartopel del evento de una interrupción no esperada.

El Plan de Recuperación de Desastres y Continuidad del Negocio, pretende cubrir los siguientes objetivos específicos:

- Recuperar la capacidad de gestión operativa en los tiempos establecidos y aceptados por la comunidad de usuarios.
- Minimizar el impacto en las áreas de negocio tanto de pérdidas financieras como de suspensión o interrupción de la capacidad operacional.

2.1.7. Consideraciones

- El plan es diseñado para recuperar la capacidad operacional desde situaciones de desastre causado por eventos externos, naturales o provocados.

- El plan se basa en el supuesto de que después del evento de desastre, existen personas que están en posibilidad de implementar los procesos de recuperación.

- El desarrollo de sistemas de información o implementación de nuevas tecnologías, podrían suspenderse dependiendo de la gravedad del evento de desastre.

- La infraestructura del Centro de Cómputo Principal podría no estar disponible total o parcialmente, por lo que las capacidades disponibles en el Centro de Cómputo Alterno deben prestar soporte para garantizar la continuidad de las operaciones.

- Se considera que los tiempos requeridos para activar el Centro de Cómputo Alterno son significativamente menores que los tiempos estimados para reparar o reconstruir el Centro de Cómputo Principal.

- Se entiende que las facilidades de Centro de Cómputo Alternos, están disponibles en el momento que se requiera ejecutar este Plan.

- Se asume que el Centro de Cómputo Alterno, no es impactado al momento del evento de desastre por otro evento en el cual puedan darse interrupciones de operación.

- La Gerencia de TI garantiza que la Institución cuenta con respaldos de la información de las operaciones que realiza día a día; y, que en cualquier momento que se requiera, dicha información está disponible para ser procesada, consultada o reinstalada de manera total o parcial.

- El tiempo de duración de la contingencia lo determina el Comité de Contingencia una vez que se ha realizado la inspección de daños ocasionados por el evento.

- Se considera que durante el tiempo que funcione el Centro Alterno, de manera paralela se está realizando la reconstrucción o reparación del Centro de Cómputo Principal para retornar cuanto antes a la normalidad.

2.1.8. Políticas de TI aplicables a la continuidad del negocio

Las políticas de Tecnología Informática establecidas por la empresa Cartopel en la que respecta la Continuidad del Negocio, son las siguientes:

Políticas Generales:

1. La empresa Cartopel, cuenta con un área responsable de la infraestructura tecnológica, que administra los bienes informáticos destinados a responder las contingencias y vigila la correcta aplicación de los procedimientos establecidos con este fin.
2. La Gerencia de TI, crea y mantiene un plan de contingencias informático, presupuestariamente ejecutable que incluye:

a. Infraestructura alterna a fin de garantizar la continuidad de las operaciones;
b. Procedimientos y mecanismos para respaldar el software e información en un lugar seguro, fuera del lugar donde habitualmente se realizan las operaciones;
c. Procedimientos y mecanismos para recuperación de software e información cuando sea necesario hacerlo.

3. Todo requerimiento de infraestructura y soluciones informáticas o equipamiento para cumplimiento de este Plan, debe ser solicitado a la Gerencia de TI por parte de los directivos de las diferentes unidades administrativas.
4. La Gerencia de TI está autorizada para emplear herramientas de Tecnología Informática y Comunicaciones que refuercen el cumplimiento de las políticas establecidas y optimicen la administración del hardware y software de la Institución.

2.1.9. Contexto del negocio

En esta sección, se identifican y analizan aquellos aspectos del negocio que están relacionados con la operatividad y funcionamiento de la entidad, esto es: políticas y objetivos de operatividad y prestación de servicio enmarcados en el plan estratégico, portafolio de productos y servicios que presta; y, procesos internos que lleva a cabo con ese fin; estos aspectos constituyen el marco de referencia para la elaboración del Plan de Recuperación de Desastres y Continuidad del Negocio:

2.1.10. Planificación Estratégica

Como una estrategia para incrementar la satisfacción del cliente, controlar los factores de riesgo operativo, con el fin de proteger y mantener un nivel adecuado de calidad en la entrega de servicios y productos a sus clientes, lo cual incluye garantizar la continuidad del servicio.

2.1.11. Identificación de la criticidad de los procesos en caso de eventos de interrupción

Asegurar claridad respecto a que áreas, procesos y actividades de la Institución serán incluidos en el PRD/CN.

Se consideran procesos críticos aquellos que en mayor o menor grado pueden impedir el normal funcionamiento de la Institución y la consecución de los objetivos planificados.

Se caracterizan porque:

- Son indispensables para garantizar la continuidad de las actividades de la empresa
- Sus funciones no pueden ser ejecutadas a menos que los recursos inhabilitados por causa de un evento, sean reemplazadas por recursos idénticos, y
- El costo de interrupción es alto y se refleja en costo de imagen y reputación y/o costos financieros.

Los tiempos máximos de recuperación con relación a los niveles de criticidad fueron establecidos en función al grado de importancia de las máquinas, equipos, sistemas entre otras herramientas que intervienen directa o indirectamente en el proceso de producción:

Nivel de Criticidad	Descripción	Tiempo máximo de recuperación
Baja	Proceso cuya falla no afecta el funcionamiento a corto plazo	1 hora – 2 horas
Media	Proceso cuya falla podría retrasar el normal funcionamiento	45 minutos a 1 hora
Alta	Proceso cuya falla podría impedir el normal funcionamiento	30 minutos a 45 minutos
Extrema	Proceso cuya falla impide el normal funcionamiento	Máximo 30 minutos

Grafico No. 2: “Niveles de criticidad de los procesos en caso de eventos de interrupción”

2.1.12. Productos que ofrece la Empresa Cartopel

La Empresa Cartopel considera que los servicios productivos de papel y empaques de cartón corrugado constituyen una verdadera solución en innovación para satisfacer las necesidades de sus múltiples clientes.

Cuenta con certificaciones internacionales de Calidad ISO 9001:2000 y forma parte de las empresas asociadas a Responsabilidad Integral (Responsabl Care), complementado de esta manera la gestión integral en áreas como la seguridad, medioambiente y salud ocupacional”.

La empresa Cartopel ofrece los siguientes materiales a la ciudadanía en general:

TIPO DE PAPEL	GRAMAJE
Corrugado Medio 127grm.	CM-127grm.
Corrugado Medio 140grm.	CM-140grm.
Corrugado Medio 155grm.	CM-155grm.
Corrugado Medio 165grm.	CM-165grm.
Corrugado Medio 175grm.	CM-175grm.
Corrugado Medio 185grm.	CM-185grm.
Kraft Linner 140grm.	kl-140grm.
Kraft Linner 160grm.	Kl-160grm.
Kraft Linner 180grm.	kl-180grm.
Kraft Linner 205grm.	Kl-205grm.
Kraft Linner 240grm.	kl-240grm.
Kraft Linner 250grm.	Kl-250grm.
Kraft Linner 270grm.	Kl-270grm.
Kraft Linner 300grm.	Kl-300grm.
Kraft Linner Intermedio 140grm.	Kl-140grm.
Kraft Linner Intermedio 160grm.	Kl-160grm.
Kraft Linner Intermedio 180grm.	Kl-180grm.
Kraft Linner Intermedio 205grm.	Kl-205grm.
Kraft Linner Intermedio 240grm.	Kl-240grm.
Kraft Linner Intermedio 250grm.	Kl-250grm.
Kraft Linner Intermedio 270grm.	Kl-270grm.
Kraft Linner Intermedio 300grm.	Kl-300grm.
Botton Pad 270grm.	BP-270
Linner Blanco 160grm.	LB-160grm.
Linner Blanco 186grm.	LB-186grm.
Linner Blanco 205grm.	LB-205grm.
Linner Blanco 230grm.	LB-230grm.
Linner Blanco 250grm.	LB-250grm.
Linner Blanco 270grm.	LB-270grm.

Grafico No. 3: “Tipos de papel que produce CARTOPEL”

2.1.13. Los sistemas de información

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.

2.1.14. Fases de un Desastre

Los desastres al estudiarlos se pueden apreciar que tienen tres fases bien definidas:

- La **etapa prepatente** es antes de empezar o manifestarse el fenómeno. Los desastres en su fase prepatente aún no se han desarrollado como tal. Los factores de riesgo están interactuando entre sí en diferentes grados de intensidad, existen los factores de riesgo interactuando o no.

  Estos factores en muchos casos pueden ser predecibles y hasta controlables. Esta fase se enfrenta o atiende con la Previsión (incluye el análisis situacional), Prevención (a nivel internacional se le llama mitigación) y Preparación (incluye la educación y la adquisición de logística).

- La **etapa patente** es cuando se propicia la con causalidad de los factores de riesgo y se desarrolla el fenómeno, impactando a la comunidad. Esta fase se enfrenta con la atención del fenómeno y su impacto.

- En la **etapa consecuencial** ya culmina o cede el fenómeno y se pueden apreciar con certeza las consecuencias del impacto. Cesa el efecto y queda el estigma del impacto o las pérdidas. Esta fase se enfrenta con la Recuperación o Rehabilitación y se comienza nuevamente en la fase Prepatente.

2.1.15. Planes de acción

2.1.15.1. 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.

2.1.15.2. Plan de emergencias

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

2.1.15.3. General – Acciones

- 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.

2.2. MARCO CONCEPTUAL

Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Se define además al plan de contingencia como un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

En la informática, un plan de contingencia es un programa alternativo para que una empresa pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez.

Estos planes también se conocen por la sigla DRP, del inglés Disaster Recovery Plan. Un programa DRP incluye un plan de respaldo (que se realiza antes de la amenaza), un plan de emergencia (que se aplica durante la amenaza) y un plan de recuperación (con las medidas para aplicar una vez que la amenaza ha sido controlada).[1]

Aristóteles, dice: “lo contingente, se contrapone a lo necesario”[2] ; es decir si se cuenta con un plan de contingencia si bien es cierto no se puede evitar ciertos desastres naturales pero se puede dar frente a ciertos incidentes fortuitos que pueden ocasionar desastres mayores con pérdidas irremediables.

---

[1] *http://definicion.de/plan-de-contingencia/*

[2] *http://www.ferratermora.org/ency_concepto_ad_contingencia.html*

2.2.1. Diferencia entre Emergencia o Contingencia, (según Elio Ríos, Copyleft 2002, Aporrea.org)

a. Es **Contingencia** (lo que puede o no suceder) si se tenía previsto por los organismos de atención y/o por la comunidad de los afectados que esto pudiera ocurrir y si se adquirió logística, se preparó personal especializado y a la comunidad para atenderlo en forma integral.

b. Es **Emergencia** el caso que este hecho no esté contemplada por los organismos de atención y/o por la comunidad de los afectados la posibilidad de aparición y desarrollo de la eventualidad, con todos los rasgo de la sorpresa y por supuesto sin tener una logística, sin preparación de personal especializado ni a la comunidad para atenderlo en forma integral.

2.2.2. Política de Seguridad

Se define como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido, en el área de seguridad durante la operación general de dicho sistema.

2.2.3. Seguridad de la Información

Se entiende como seguridad de la información a la preservación de las siguientes características:

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución.

- **Auditabilidad**: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

- **Confiabilidad de la Información:** Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.[3]

2.2.4. Desastre

El autor Elio Ríos, define al "desastre como cualquier hecho o fenómeno que desemboca en la alteración de la integridad de los humanos, su sociedad, sus bienes y/o los factores naturales en una comunidad y en una localidad determinada, dando un rendimiento de pérdidas, alterando el desarrollo normal de las actividades actuales y futuras de humanos, sus formas de organización o del ambiente."

Un desastre ocurre cuando se correlacionan un fenómeno (impacto) y las condiciones de vida de una población habiendo un saldo negativo para el segundo (vulnerabilidad). Mientras más factores de riesgos coincidan en una misma zona, más oportunidad que se desarrolle un desastre, además de mayor efecto sobre esa comunidad.

Es una situación resultante en una sociedad o comunidad, después que ha sido azotada por algún fenómeno natural, llámesele: terremoto, inundación, huracán, vulcanismo, deslizamiento u otro; o por acciones erróneas del hombre, tales pueden ser los casos de incendios, explosiones etc. En ambos casos, el desastre se puede medir en términos de daños y pérdidas materiales, económicas; o en lesiones y pérdidas de vidas humanas.

2.2.5. Clasificación de los desastres

Los desastres se pueden clasificar de acuerdo a diferentes variables; algunas de éstas son:

a. Por su aparición:

[3] *es.wikipedia.org/wiki/Plan_de_Contingencias*

- **Súbitos**: Son aquellos fenómenos que ocurren sorpresivamente y de manera inmediata. Por ejemplo: terremotos, avalanchas, algunas inundaciones, tsunamis (maremotos).

- **Mediatos**: Se desarrollan en forma más lenta y es factible predecirlos: por ejemplo: Huracanes, sequías erupciones volcánicas y otros.

b. Por su duración:

- **Corta a mediana duración:** Terremotos, huracanes, erupciones volcánicas, tsunamis, avalanchas y hundimientos.

- **Larga duración:** Sequías, epidemias e inundaciones.

c. Por su origen:

- **Naturales**: Son los que se originan por la acción espontánea de la vida misma de la naturaleza o de la evolución del planeta.

- **Incendios:** Son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad de las computadoras, ya que puede destruir fácilmente los archivos de información y programas.

- **Inundaciones**: en las épocas de lluvia aumenta el caudal de los ríos y/o los cauces de aguas de las ciudades (cañadas) pueden desbordar sus aguas y arrasar las propiedades, los cultivos, los animales y hasta seres humanos (pérdidas). Esto conlleva al desplazamiento en forma de evacuación y a pérdidas antedichas.

- **Terremotos**: El desplazamientos de las placas tectónicas causa cúmulos de energía en forma de tensión las cuales al liberarse hacen que se deslicen capas de la tierra con propagación de la onda. Esta vibración puede dañar las edificaciones en diferentes grados y a otros factores de nuestra comunidad. Estas pérdidas también incluyen a los humanos el cual se afecta en forma biológica, síquica y social.

Inducidos: Son aquellos que fundamentalmente se desarrollan por error del hombre o abuso que éste hace en la explotación de los recursos que le proporciona la natural.[4]

- **Robo Informático.-** Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina, debido a esto la información importante o confidencial puede ser fácilmente copiada sin dejar ningún rastro. (explicativo)

- **Fraude Informático.-** Por esta causa millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien que perder en imagen, no se da ninguna publicidad a este tipo de situaciones.

- **Sabotaje Informático.-** El peligro más temido en los centros de procesamiento de datos, es el sabotaje, los imanes son las herramientas a las que se recurre con una ligera pasada del imán la información desaparece.

2.2.6. Impacto

El impacto es el alcance cuantificado y calificado del daño ocasionado por un desastre. El impacto se puede valorar como de mayor o menor magnitud, depende de las características del fenómeno y así también del punto de vista de la vulnerabilidad en la comunidad. Un plan de contingencias es bueno para evitar o disminuir este impacto.

2.2.7. Vulnerabilidad

La vulnerabilidad es la capacidad de un recurso (humano, social, cultural, material, ambiental, agropecuario, transporte, financiero, económico, estructural, habitacional, etc.) o de una comunidad, de ser dañado por la ocurrencia de un fenómeno (natural, tecnológico, social, cultural, deportivo, económico, epidemiológico). La debilidad o incapacidad de una comunidad para evitar, resistir y recuperarse de un desastre. Es el grado de pérdida de un recurso o de una comunidad si es sometido a la acción de un fenómeno.

---

[4]www.binasss.sa.cr/poblacion/desastres.htm

2.2.8. Daño o pérdida

El daño o pérdida es el perjuicio, lesión, detrimento, la disminución parcial o total de la masa o de la función o de su posesión debido a extravío, destrucción, amputación, perecimiento, pérdida de un vínculo, afectación pública debido a la acción u omisión o cese de un fenómeno. Es la muerte, privación, desaparición o daño de factores componentes de una comunidad. Es el daño total o parcial, temporal o permanente, la desaparición de un recurso (humano, social, cultural, material, ambiental, agropecuario, transporte, financiero, económico, estructural, habitacional, etc.).

2.3 MARCO ESPACIAL

El estudio de un plan de contingencia contra desastres informáticos lo realizaré dentro del área de producción en la Empresa Cartopel S.A.I. ubicada en el sector del Parque Industrial.

CAPITULO III

3. METODOLOGÍA

3.1. Metodología de investigación

3.1.1. Unidad de Análisis

El análisis está enfocado en el área de producción en la Empresa Cartopel S.A.I., que es una empresa privada cuyo finalidad es la producción de papel al servicio de la ciudadanía, y que luego de análisis exhaustivo se ha detectado la necesidad de disponer de mecanismos para garantizar la confidencialidad, integridad y seguridad de los mismos, para el efecto se ha analizado la necesidad imperiosa de realizar un estudio para implementar políticas de seguridad informáticas que permitan dar frente a los diferentes riesgos sean estos provocados o de carácter natural y que puedan amenazar el normal funcionamiento de la empresa.

3.1.2. Tipo de Investigación

Con el desarrollo de este proyecto se hará uso de la metodología investigativa que pretende brindar mayor seguridad en la información de la empresa y brindar una mayor efectividad mediante un plan de contingencia contra desastres; así mismo se pretende proteger la parte económica ya que al realizar el estudio previo la inversión en software y hardware es muy alta debido al costo de los equipos y el sistema.

El tipo de investigación que utilizaremos será el descriptivo ya que por motivos de tiempo para la entrega de este análisis no es muy extenso.

3.1.3. Técnicas de Investigación

Para la investigación que se va a realizar utilizare básicamente dos técnicas básicas.

Observación: Consiste en observar personas, fenómenos, hechos, casos, objetos, acciones, situaciones, etc., con el fin de obtener determinada información necesaria para una investigación.

Recopilación: Se refiere al uso de una gran diversidad de técnicas y herramientas que pueden ser utilizadas por el analista para desarrollar los sistemas de información, los cuales

pueden ser la entrevistas, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos.

Cabe indicar que el objeto de la investigación descriptiva consiste en evaluar ciertas características de una situación particular en uno o más puntos del tiempo. En esta investigación se analizan los datos reunidos para descubrir así, cuales variables están relacionadas entre sí.

CAPITULO IV

4. DESARROLLO

4.1. IDENTIFICACIÓN DE RIESGOS

El propósito de esta etapa es por una parte identificar las causas potenciales de interrupción de las actividades de la Institución, la probabilidad de ocurrencia y el impacto que tendría la amenaza de llegar a darse. Por otra parte, se trata de obtener comprensión de los procesos más críticos de la Institución, cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la Institución.

4.1.1. Objetivos específicos de esta etapa:

- Identificar y valorar los riesgos de interrupción de la capacidad operacional
- Valorar el impacto de los eventos de riesgo en el proceso de producción
- Valorar el impacto de los eventos de riesgo en la tecnología
- Determinar las prioridades y tiempos de recuperación de los sistemas de información

4.1.2. Supuestos

Los siguientes supuestos se aplican en esta etapa:

- El análisis y calificación de riesgos se realiza para los procesos identificados como críticos (en nivel alto y extremo) en la etapa anterior.
- La valoración de riesgos se realiza en base a información recopilada tanto de estudios realizados anteriormente como de registros históricos y criterios de los directivos que participan en las reuniones.
- Los resultados de esta etapa, reflejan los hallazgos encontrados a la fecha de presentación de este estudio.

El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas.

En la empresa CARTOPEL S.A.I, se han determinado varios riesgos de seguridad general que afectan informáticamente, entre otros:

Grafico No. 4: "Riesgos que pueden presentarse para la empresa"

4.1.3. Eventos Naturales

El cuidado y la preocupación de los riesgos originados en desastres naturales se han incrementado durante los últimos años. Cartopel en este capítulo del estudio, identifica estas exposiciones, evalúa su gravedad y posible impacto, así como las estrategias de manejo y planes de acción para control de estos eventos.

Estos riesgos tienen su origen en la naturaleza por lo que prevenir su presencia e impacto es muy difícil. Los riesgos a que está expuesta la Entidad, se clasifican de la siguiente manera:

a) Inundación: Son los daños ocasionados por el cubrimiento de un lugar con agua.

b) Incendio: Corresponde a los daños ocasionados por fuego de grandes proporciones que destruye lo que no está destinado a arder.

c) Terremoto: Es la agitación violenta o sacudida del terreno, ocasionada por fuerzas que actúan en el interior del globo terrestre.

Suspensión de las actividades necesarias para operación de equipos, maquinarias y otras herramientas utilizadas en las actividades de producción y de los funcionarios. Se clasifican en:

d) Falla Eléctrica: Es la falta de suministro de energía que impide el funcionamiento de equipos y herramientas para la operación dentro de las organizaciones.

e) Falla Térmica: Es la variación de la temperatura en los equipos informáticos que se encuentran en la sala de control que impide el funcionamiento de equipos y herramientas para la producción.

Incidentes de Seguridad de la Información

Situaciones de emergencia ocasionadas por una administración de seguridades de información no adecuada, así como por falta de políticas integrales de seguridad y monitoreo de accesos de las redes de comunicación y accesos a los sistemas de la Institución. Se clasifican en:

f) Compartir Contraseñas: Es la revelación de información sensible en forma no autorizada y premeditada, lo que ocasiona accesos indebidos.

g) Mal uso del sistema: Personas no autorizadas y sin capacitación debida utilizan los equipos informáticos.

La matriz de eventos de riesgo se construye a partir de dos ejes: probabilidad de ocurrencia de los eventos de riesgo y el impacto en la Institución.

4.1.4. Probabilidad

Es la posibilidad de ocurrencia de un evento específico o resultado, medido por la relación de eventos específicos o resultados ocurridos sobre el número total de posibles eventos o resultados.

Este criterio se ha clasificado en tres categorías.

4.1.5. Matriz de Riesgos

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente:

MATRIZ DE RIESGOS											
ELEMENTOS DE INFORMACION	PROBABILIDAD DE AMENAZA										
	MAGNITUD DE DAÑO	CRIMINALIDAD		SUCESOS FISICOS					NEGLIGENCIA		
		USO MALICIOSO	VIRUS	INCENDIOS	INUNDACIONES	TERREMOTOS	FALLAS TERMICAS	FALLAS ELECTRICAS	COMPARTIR CONTRASEÑAS	MAL USO DEL SISTEMA	FALTA DE CAPACITACION SOBRE RIESGOS
EQUIPOS INFORMATICOS	ALTO	1	2	5	4	1	4	3	2	3	3
SERVIDORES	ALTO	2	2	5	4	1	5	3	1	1	3
TERMINALES	ALTO	1	2	5	4	1	3	3	1	2	3
REDES DE DATOS	CATASTROFICO	3	2	5	4	1	3	3	2	2	2
INFORMACION	CATASTROFICO	2	2	5	4	1	3	3	2	3	2
EDIFICACION	MODERADO	1	2	5	4	1	3	2	1	1	1

Impacto:
1 = Insignificante
2 = Menor
3 = Moderado
4 = Alto
5 = Catastrófico

Probabilidad:
1 = Muy baja
2 = Baja
3 = Moderado
4 = Alta
5 = Muy Alta

Grafico No. 5: "Matriz de Riesgos Probabilidad Amenaza vs. Magnitud de Daño"

4.2. IMPACTO

Es el nivel de afectación en uno o más objetivos institucionales debido a un evento de riesgo.

Los parámetros y medidas utilizados para construir la matriz de riesgos corresponden a técnicas de evaluación cualitativas que proporcionan una forma de priorizar y otorgar importancia relativa a los riesgos utilizando escalas descriptivas.

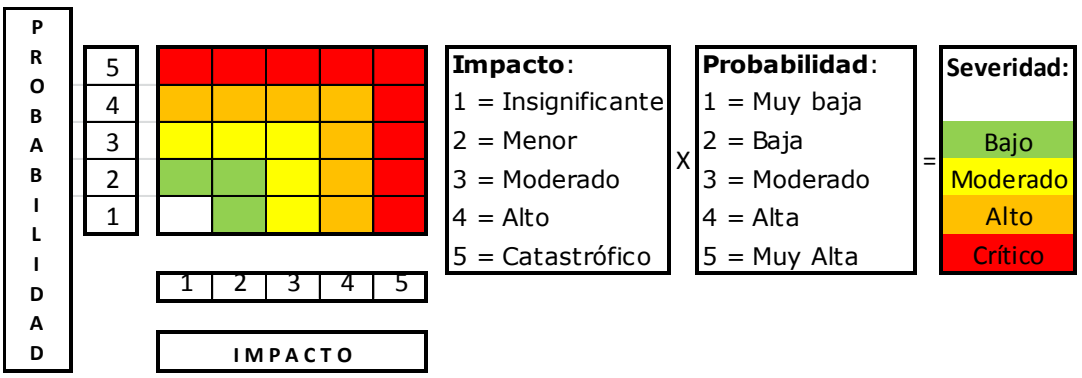

Grafico No. 6: "Parámetros para medir riesgos"

PROBABILIDAD	
Valoración	**Descripción**
Muy baja	Al menos una vez en los cuatro últimos años
Baja	Al menos una vez en los tres últimos años
Moderada	Al menos una vez en los dos últimos años
Alta	Al menos una vez al año
Muy alta	Al menos una vez al trimestre

Grafico No. 7: "Valoración de la probabilidad"

IMPACTO	
Valoración	**Descripción**
Insignificante	▪ Riesgo de inconvenientes menores ▪ Riesgo de demoras en actividades de la empresa
Menor	▪ Riesgo de inconvenientes significativos ▪ Riesgo de disminución de utilidades de la empresa
Moderado	▪ Riesgo de demoras significativas en operaciones ▪ Riesgo de infracciones a la regulación ▪ Riesgos de pérdida de oportunidades de la empresa
Alto	▪ Riesgo de alteración, corrupción o pérdida de datos ▪ Riesgo de interrupción de una parte de las operaciones
Catastrófico	▪ Riesgo de continuidad del proceso de producción y como consecuencia la pérdida de clientes o ingresos. ▪ Riesgo de exposición significativa a quejas importantes por incumplimiento o demanda de clientes

Grafico No. 8: "Valoración del impacto"

4.3. VALORACIÓN DEL IMPACTO DE LOS EVENTOS DE RIESGO EN LOS PROCESOS

4.3.1. Consideraciones

Los resultados de la valoración del impacto de los eventos de riesgo en los procesos de la Institución, se aplican tanto para la construcción del Plan de Recuperación de Desastres y

Continuidad de la Empresa como para el análisis, diseño e implementación del Centro de Cómputo Alterno.

4.3.2. Proceso Críticos

La valoración del impacto de los eventos de riesgo en los procesos de la Institución, se inicia con el reconocimiento de la ubicación física de los procesos calificados como críticos y el análisis de las prestaciones y seguridades de los edificios donde se desarrollan dichas actividades.

El siguiente cuadro muestra la ubicación física de los procesos calificados como críticos:

TIPO DE PROCESO	PROCESO CRITICO	UNIDAD ADMINISTRATIVA	UBICACIÓN FISICA
PRODUCCIÓN	• PREPARACIÓN DE PASTA	SUPERINTENDENCIA DE PRODUCCIÓN	PLANTA DE PRODUCCIÓN, PARTE EXTERIOR - POSTERIOR
	• PROCESO DE REFINACIÓN		NAVE – SEGUNDO PISO INTERIOR
	• PROCESO DE FORMACIÓN		
	• PROCESO DE SECADO.		
	• PROCESO DE TERMINADO		
	• PROCESO DE DESPACHO	JEFATURA DE DESPACHOS	NAVE – PRIMER PISO INTERIOR

Grafico No. 9: “Procesos Críticos de la empresa”

En la empresa Cartopel se cuenta con una nave de producción.

4.3.3. Valoración del Impacto de Eventos Naturales

La valoración de los eventos de riesgo se ha realizado teniendo en cuenta la información disponible respecto de los daños causados por la sucesión de eventos naturales, principalmente con riesgos relacionados por inundaciones incendios y terremotos y las características de los edificios.

Evento	Definición	Probabilidad	Impacto
NATURALES	Inundación	4. Alta	Alto
	Incendio	5. Muy Alta	Catastrófico
	Terremoto	1. Muy Baja	Catastrófico

Grafico No. 10: "Eventos naturales probabilidad vs impacto"

La evaluación del **riesgo de inundaciones** se realiza a partir de los antecedentes ocurridos en la empresa Cartopel, por cuanto uno de los principales recursos para la producción del papel es el agua y se la provee desde el río, por otro lado la cubierta de la infraestructura de la Nave de producción es eternit material que no proporciona un 100% de seguridad frente a lluvias fuertes, así mismo se trabaja con vapor el mismo que se condensa en la cubierta produciendo humedad interior en grandes cantidades, afectado el proceso de producción y a los recursos materiales, tecnológicos, entre otros. Con estos antecedentes se califica la probabilidad como "alta" y el impacto "alto".

Para evaluar el **riesgo de incendio** se toma en cuenta que la materia prima que se utiliza en este proceso es 100% inflamable (papel, cartón). En base a la información disponible, se califica la probabilidad como "muy alta" y el impacto "catastrófico".

La evaluación del **riesgo de terremoto** se realiza a partir de la revisión de registros de sucesos similares y de los cuales no existe información histórica. En el mapa de riesgo, se califica la probabilidad como "muy baja" y el impacto "catastrófico".

4.3.4. Valoración de Impacto de Pérdida de Servicios

Evento	Falla	Probabilidad	Impacto
PERDIDA DE SERVICIOS	Eléctrica	Alta	Moderado

Grafico No. 11: "Pérdida de Servicios probabilidad vs impacto"

La evaluación del **riesgo de pérdida de servicios de electricidad** se realiza a partir del análisis de los cortes de energía eléctrica que generalmente se han dado de manera eventual por fallas temporales o mantenimiento.

Sin embargo en noviembre del 2009 se realizaron cortes por racionamiento de energía que se extendieron por más de 60 días.

Sin embargo, Cartopel cuenta con un generador de energía de alta potencia con mayor carga operativa. Con estos antecedentes se califica la probabilidad como "alta" y el impacto "moderado".

4.3.5. Valoración del Impacto de Fallas en Equipos y Sistemas:

Evento	Falla	Probabilidad	Impacto
FALLAS DE EQUIPOS	Térmica	Alta	Moderado

Grafico No. 12: "Falla de Equipos probabilidad vs impacto"

La evaluación del **riesgo de falla térmica** se realiza a partir de los antecedentes ocurridos por daño en el sistema de aire acondicionado. Con estos antecedentes se califica la probabilidad como "alta" y el impacto "moderado".

4.3.6 Valoración del Impacto de Incidentes de Seguridad de la Información

Evento	Definición	Probabilidad de Ocurrencia	Impacto
INCIDENTES DE SEGURIDAD	Accesos Indebidos	Baja	Menor
	Pérdida de datos	Baja	Alto
	Falla en los Sistemas Informáticos	Moderada	Alto

Grafico No. 13: "Incidentes de Seguridad probabilidad vs impacto"

No se han dado eventos de **accesos indebidos** y no se cuenta con registros. En el mapa de riesgo, se califica la probabilidad de estos eventos como "baja" y el impacto "menor".

La **pérdida de datos** por fallas de procesamiento se ha dado eventualmente aunque no se tienen registros. En el mapa de riesgo, se califica la probabilidad de estos eventos como “baja” y el impacto “alta”.

La **falla de sistemas informáticos** se ha dado eventualmente aunque no se tienen registros. En el mapa de riesgo, se califica la probabilidad de estos eventos como “moderada” y el impacto “alto”.

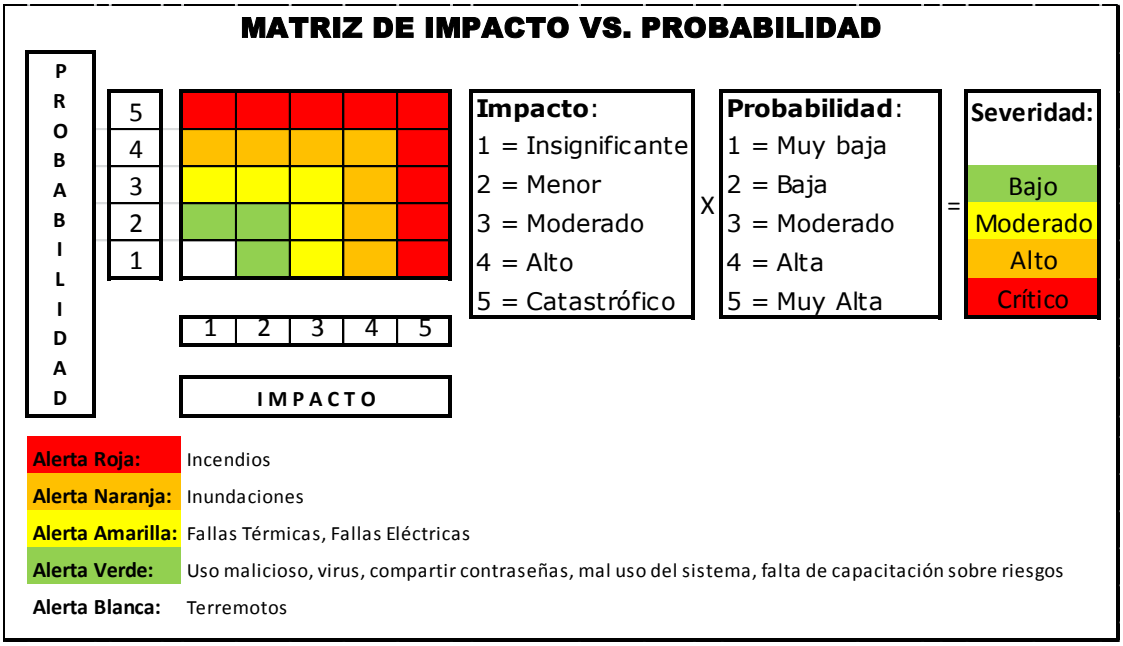

Grafico No. 14: “Matriz de probabilidad vs impacto”

4.4. ESTUDIO DEL PLAN DE CONTINGENCIA QUE SE PROPONDRÁ A LA EMPRESA

4.4.1. Definir estrategia

Pese a todas las medidas de seguridad puede ocurrir un desastre es por este motivo que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", "por si ocurre algún desastre natural” o “por si existe algún tipo de criminalidad”.

Por tanto, es necesario dar un primer paso para realizar un análisis de un Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

4.4.2. Objetivo de la Etapa

El propósito de esta etapa es identificar las estrategias y métodos operativos que serán aplicados en la Institución para disminuir la exposición al riesgo de interrupción de las actividades de producción.

4.4.3. Objetivos específicos de esta etapa:

- Definir las políticas, estrategias y dirección del Plan de Continuidad del Cartopel.

4.4.4. Estrategias Corporativas

En esta sección se analizan las estrategias de manejo de riesgo adecuadas para cada evento identificado y evaluado.

Se consideran las siguientes estrategias de manejo de riesgos:

- **Reducir**: implantación y actualización de controles para minimizar el riesgo y mantenerlo a un nivel aceptable.
- **Aceptar**: cuando el coste de las medidas sea mayor que las consecuencias de la materialización del riesgo.
- **Transferir**: contratar pólizas de riesgo.

Para este efecto se ha propuesto a la Empresa Cartopel realizar las siguientes acciones de recuperación de desastres:

Tipo de Evento	Evento	Probabilidad Ocurrencia	Impacto	Estrategia de Manejo	Solución Adoptada
Eventos Naturales	Inundación	Alta	Alto	Reducir	▪ Resguardar documentos valorados en cajas de seguridad para garantizar niveles de protección adecuados. ▪ Aplicar buenas prácticas de estandarización de trabajo y digitalización de la información sensitiva. ▪ Estrategias de respaldo y recuperación de información.
	Incendio	Alta	Catastrófico	Reducir y Transferir el Riesgo	▪ Mantenimiento y verificación de sistema de prevención contra incendio ▪ Contrato de seguro contra incendios para el edificio. ▪ Resguardar documentos valorados en cajas de seguridad para garantizar niveles de protección adecuados. ▪ Aplicar buenas prácticas de estandarización de trabajo y digitalización de la información sensitiva. ▪ Estrategias de respaldo y recuperación de información. ▪ Uso del Centro de Cómputo Alterno en caso de daño en el Centro de Cómputo Principal. ▪ Procedimiento y brigadas contra incendios
	Terremoto	Baja	Catastrófico	Reducir	▪ Resguardar documentos valorados en cajas de seguridad para garantizar niveles de protección adecuados.

Tipo de Evento	Evento	Probabilidad Ocurrencia	Impacto	Estrategia de Manejo	Solución Adoptada
					▪ Aplicar buenas prácticas de estandarización de trabajo y digitalización de la información sensitiva. ▪ Estrategias de respaldo y recuperación de información. ▪ Establecer Centro de Cómputo Alterno en caso de daño de Cómputo Principal.
Fallas en Equipos y Sistemas	Falla Eléctrica	Moderado	Moderado	Reducir	▪ Se cuenta con un generador de energía alterno. ▪ Mantenimiento continuo
	Falla Térmica	Moderado	Moderado	Reducir	▪ Contrato de mantenimiento de aire acondicionado en la nave
Eventos Provocados	Uso Malicioso	Muy Baja	Moderado	Reducir	▪ Resguardar documentos valorados en cajas de seguridad que aseguren niveles de protección adecuados. ▪ Aplicar buenas prácticas de estandarización de trabajo y digitalización de la información sensitiva. ▪ Estrategias de respaldo y recuperación de información. ▪ Procedimientos y sistemas de seguridad física
Incidentes de Seguridad de la Información	Virus	Baja	Moderado	Reducir	▪ Software para detectar y controlar virus informáticos en servidores y PC's. ▪ Estrategias de respaldo y recuperación de información.
	Mal uso del Sistema	Bajo	Alto	Reducir	▪ Estrategias de respaldo y recuperación de información. ▪ Capacitación a los usuarios del sistema

Tipo de Evento	Evento	Probabilidad Ocurrencia	Impacto	Estrategia de Manejo	Solución Adoptada
	Compartir contraseñas	Baja	Moderado	Reducir	▪ Capacitar en la reserva del Login single/sign on ▪ Procedimientos para manejo de claves
	Falta de capacitación sobre riesgos	Moderado	Alto	Reducir	▪ Inducir para que dentro del plan de capacitación se incluya el tema relacionado con los diferentes riesgos que pueden presentarse. ▪ Incluir todo tipo de señalética de prevención y cuidado de equipos, información y otros riesgos a presentarse.

Grafico No. 15: “Acciones de Recuperación de Desastres”

4.5. ESTRATEGIA DE TECNOLOGÍA DE LA INFORMACIÓN

La Empresa Cartopel deberá definir un Centro de Cómputo Alterno de tal manera que se pueda prevenir cualquier incidente en este espacio y con el fin de precautelar la información y los sistemas que permiten el desarrollo del proceso de producción en la fábrica.

Se recomienda además, tener duplicidad en los respaldos, los mismos que deberán ser resguardados y mantenerse “in situ” es decir en la empresa para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.

Todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Empresa Cartopel, serán creados copias de Seguridad, para lo cual se debe contar con:

- Backups del Sistema Operativo.
- Backups del Software Base - Paquetes y/o Lenguajes de Programación.
- Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes)
- Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados)
- Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como ambiente y facilidades de trabajo.

4.6. RESPUESTA OPERATIVA

4.6.1. Políticas y Consideraciones a tener en cuenta

- Los procesos calificados como críticos y que deben atenderse con prioridad en caso de un evento de desastre son:

PROCESO	UNIDAD ADMINISTRATIVA
Producción	Superintendencia de producción

Grafico No. 16: “Proceso prioritario a atenderse en caso de siniestro”

- El desarrollo del Plan de Continuidad en un evento de desastre no tendrá en lo posible una duración mayor a 8 días calendario dependiendo el desastre, periodo en el cual se pretende restablecer el Centro de Cómputo para retornar a la normalidad.

- Mantener permanentemente actualizados los registros informáticos que hacen referencia a documentos valorados, contribuye a disminuir los riesgos operativos en este aspecto.

- Otros procesos que se desarrollan, como: administrativos, bodega, entre otros podrán ser suspendidos mientras dura la contingencia, dependiendo del impacto del evento.

- Las personas que trabajan en los procesos calificados como críticos y cuyas áreas han sufrido daños, deben trasladarse físicamente a otras oficinas para el desempeño de sus tareas. El Gerente de esa oficina velará por la disposición de recursos y materiales para el desarrollo de sus actividades.

- El personal de la nave de producción que trabaja en el control, procesamiento y desarrollo de producción de la Empresa Cartopel, deberá trasladarse a un centro alterno, donde dispondrá de estaciones de trabajo, conectividad, equipos y recursos para el desarrollo de sus actividades.

- Debido a que él Plan de Continuidad se enfoca a la protección del personal, recuperación de los espacios físicos y recuperación de servicios de TI en caso de un evento de desastre, los procesos de apoyo que están relacionados con estos objetivos se consideran críticos. (servicios generales, seguros, pagos, pasajes, viáticos, etc.).

- El Grupo de Continuidad, tomará las decisiones de acuerdo al grado de severidad del evento e informará internamente de las políticas que aplicarán para control del evento, activación y desactivación del Plan de Continuidad.

4.7. CENTRO DE CÓMPUTO ALTERNO

4.7.1. Características Físicas

El Centro de Cómputo Alterno, dispone de:

- Sitio físico expresamente acondicionado para esta función
- Sistema y servicios de energía eléctrica alterna
- Sistema y servicios de seguridad física
- Sistema y servicio contra incendios

4.7.2. Escenario de Recuperación

El enfoque propuesto para la implantación del Plan de Continuidad de Servicio, considera la replicación de dos elementos simultáneos en tiempo real de la información, incluye replicación de las bases de datos, servidores de aplicaciones, sistema de mensajería y correo electrónico, servidores de dominio, software de administración de red y máquinas virtuales.

Para implementar la solución de Virtualización se crearon cluster de servidores Blade, que funcionan de manera independiente al cluster de servidores Blade para bases de datos.

Por otro lado, la empresa Cartopel, seleccionó como alternativa tecnológica de recuperación, la modalidad denominada: Dos fases en Dos sitios. Se define por poseer un centro alterno con hardware completamente dedicado (segundo sitio), con capacidad para mantener y sincronizar tanto los datos como las aplicaciones a más de la disponibilidad de enlaces redundantes con amplio ancho de banda entre los sitios.

Los datos y aplicaciones críticas están presentes en ambos sitios, asegurando una reconexión rápida de las redes y aplicaciones, minimizando al máximo el tiempo de recuperación.

Las oficinas de la Institución, suspenderán momentáneamente sus actividades durante el tiempo de conexión al sitio alterno. Una vez que entre en funcionamiento continuarán sus actividades, de acuerdo a los procedimientos que para ello establezca la Gerencia de Tecnología de la Información.

4.7.3. Seguridades

El área de Tecnología proporcionará en el Centro Alterno, servicios de administración del Firewall, detección y prevención de intrusos (IDS e IPS), filtrado de contenido Web, Antivirus y Antispam.

4.8. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN

4.8.1. Alcance

La estrategia de respaldo tiene el siguiente alcance:

- Datos de las aplicaciones centralizadas
- Datos almacenados en las estaciones de trabajo de los usuarios y que han solicitado respaldo
- Sistemas Operativos, software de escritorio y aplicaciones centralizadas
- Servicios de Correo electrónico y Web
- Comunicaciones IP

4.8.2. Datos de aplicaciones centralizadas

Respaldo Total (full backup) para datos de aplicaciones centralizadas

Se aplica a los datos ubicados en servidores del Centro de Cómputo; todos los datos se respaldan diariamente.

Archivos de Respaldo

Al menos dos copias deben realizarse de los datos. Una copia física se almacena en el Centro de Cómputo bajo procedimientos de seguridad definidos.

La copia generada mediante procesos de replicación está ubicada en el Centro de Cómputo Alterno de acuerdo a los procedimientos de seguridad implementados.

Pruebas

Una vez al mes, el operador del Centro de Cómputo realizara pruebas de funcionamiento de los respaldos que mantiene en ese lugar.

Diariamente el operador del Centro de Cómputo Alterno realiza pruebas de funcionamiento de los respaldos obtenidos mediante el proceso de replicación, de acuerdo al procedimiento definido.

4.8.3. Datos almacenados en las estaciones de trabajo de los usuarios

Para el respaldo de la información almacenada en las máquinas de los usuarios, es necesario que el funcionario solicite a Seguridad de la Información este servicio.

Luego de aceptada la solicitud, personal de Seguridad de la información procederá a instalar los agentes de respaldo en la máquina del funcionario y definir conjuntamente la información que debería ser respaldada al igual que su frecuencia.

Una vez definido e instalado el Agente se deberá comunicar con el funcionario responsable de la Administración y Operación de respaldos para que proceda con la implementación.

Respaldo Total o Diferencial para servidores de archivo

El proceso se aplica a los archivos que han sido requeridos para respaldo por parte de los usuarios según el procedimiento establecido.

Los archivos se respaldan con la frecuencia indicada en el procedimiento, manteniendo un respaldo original en el Centro de Cómputo Principal y una copia en el centro de cómputo alterno.

Se realiza un respaldo al inicio y en lo posterior son respaldos incrementales, de esta manera se optima recursos de Cinta y de procesamiento, garantizando completa seguridad.

Archivos de Respaldo

El Respaldo Original se encuentra ubicado en el Centro de Cómputo, bajo procedimientos de seguridad establecidos.

La copia generada automáticamente está ubicada en el Centro de Cómputo Alterno bajo procedimientos de seguridad establecida.

Pruebas

Semanalmente el Administrador de respaldos junto con el oficinal de Seguridad de la información realiza pruebas de restauración de los archivos respaldados.

Una vez al mes el operador del Centro de Cómputo Alterno realizará pruebas de recuperación de los respaldos obtenidos de acuerdo al procedimiento anterior.

4.8.4. Sistemas Operativos de Red y Aplicaciones

Respaldo de sistemas operativos de red y aplicaciones

Para los sistemas operativos, de red y aplicaciones (incluye: Internet, Correo Electrónico, Swift y Web), se realizará control de cambios e instalación de versiones.

Los sistemas operativos de red y aplicaciones se respaldarán una vez que hayan sido instalados configurados y probados, es decir cada vez que haya cambios.

El proceso de respaldo se realizará mediante replicación y de acuerdo al procedimiento descrito.

Archivos de Respaldo

La copia generada mediante procesos de replicación es ubicada en el Centro de Cómputo Alterno.

Pruebas

Una vez al mes el operador del Centro de Cómputo Alterno realizará pruebas de funcionamiento de los respaldos obtenidos por replicación.

4.8.5. Tiempos de Recuperación

La siguiente tabla muestra los tiempos promedios de recuperación de la infraestructura tecnológica en el sitio alterno:

TAREA	TIEMPO DE DURACIÓN (horas)
Declaración de Contingencia y Organización	
Sistemas Centralizados	
• Levantar Sistemas Operativos y de Red	25 min
• Verificar Configuraciones	50 min
• Levantar Aplicaciones	25 min
• Verificar Configuraciones y Versiones	25 min
• Restaurar Datos	25 min
• Verificar Integridad	1 hora
Comunicaciones WAN – LAN	
• Instalar el S.O.	30 min
• Revisar Configuraciones y Habilitar	30 min
Tiempo de Recuperación por Estación:	**4 horas 30 min**

Grafico No. 17: "Tiempos de Recuperación de la Infraestructura tecnológica"

Es necesario indicar que los tiempos de recuperación de la infraestructura tecnológica se han establecido en base a la experiencia por incidentes presentados durante los 20 años de funcionamiento de la fábrica Cartopel, los mismos que han sido remediados por el departamento de Tecnologías de la Información - TI y que constan en bitácoras del proceso.

4.8.6. Brecha de Recuperación y Soluciones

La brecha de recuperación representa la diferencia de tiempo existente entre la capacidad actual de recuperación de Tecnología de la Información y los tiempos de recuperación tolerables por parte de los procesos que requieren de las aplicaciones para su funcionamiento.

El tiempo de activación del centro de cómputo alterno, tomando en cuenta actividades técnicas de control del evento y considerando que existen facilidades administrativas para que personal se desplace a otras oficinas de la ciudad para desarrollar sus actividades, es de 3,30 horas.

Debido a que no todas las estaciones de trabajo se deben recuperar en su totalidad, los tiempos de restauración de las PC's están considerados dentro del mismo margen de tiempo considerado para la restauración del centro de cómputo alterno.

La brecha de recuperación se ubica en 1 hora y 45 minutos, que para un evento de desastre cuya solución amerita al menos 24 horas de suspensión de servicios, Cartopel considera dicha brecha tolerable.

4.9. PROCEDIMIENTO DE EMERGENCIA

4.9.1. Responsabilidades del Equipo de Continuidad

Conformado por las siguientes personas:

- Superintendente de Producción,
- Jefe de Producción,
- Ingeniero en Procesos,
- Director Administrativo (Líder de Brigadas Contraincendios), y
- Un Delegado de Riesgos.

El Superintendente de Producción, es el Coordinador del Equipo de Continuidad.

Este equipo de trabajo es parte del grupo staff o equipo de continuidad de la Empresa con quienes se coordinan las actividades en su ámbito de responsabilidad y en el marco de trabajo establecido.

Las principales actividades y responsabilidades son las siguientes:

ACTIVIDADES	RESPONSABLES
Mantener vigente el Plan de Continuidad de la Empresa y coordinar la realización de pruebas periódicas.	Equipo de Continuidad en coordinación con las Unidades Administrativas.

Desarrollar acciones y proveer de recursos para la implementación del Plan de Recuperación de Desastres y Continuidad de la Empresa.	Equipo de Continuidad en coordinación con las Unidades Administrativas.
Asegurar existencia, exactitud, preservación y accesibilidad de los documentos del plan de continuidad.	Equipo de Continuidad
Mantener control de la información y documentos de la empresa.	Unidades Administrativas con asistencia de TI
Monitorear el desarrollo del Plan, revisar los resultados de las pruebas y hacer sugerencias de mejora.	Auditoria Interna y Directivos.
Activar el Plan en caso de evento de desastre y coordinar el desarrollo de actividades antes, durante y después del evento.	Equipo de Continuidad

Grafico No. 18: "Principales actividades vs. Responsables"

4.9.2. Escalabilidad de Eventos

La decisión de utilizar el sitio alterno depende de dos factores:

- El tiempo de la interrupción
- El segmento o parte del ciclo de la empresa que está involucrado en la interrupción.

Dependiendo de estos dos factores se han establecido planes de escalamiento en base a la matriz de análisis de impacto y a las disponibilidades tecnológicas de la Institución:

Plan 1	Cuando la valoración del daño indica que el impacto es parcial y que la recuperación es posible en 24 horas o menos. El Equipo de Continuidad coordina la recuperación en la misma localidad.

Plan 2	Cuando la valoración del daño indica que el impacto es parcial o total y la recuperación tomará más de 24 horas. El Equipo de Continuidad coordina la activación del Centro Alterno y la reubicación de las Unidades Administrativas afectadas si es del caso. El peor escenario de contingencia se considera la interrupción de la continuidad de la empresa por falta de actividad del Centro de Cómputo Principal y la necesidad de desplazamiento del personal de las Unidades Administrativas hacia otras localizaciones para desarrollar su trabajo.

Grafico No. 19: "Escalabilidad de Eventos"

4.9.3. Acciones preventivas de las Unidades Administrativas

Todas las dependencias de la Empresa Cartopel deberán tomar en cuenta las siguientes políticas para disminuir los riesgos y garantizar la continuidad de las actividades:

- Adoptar estándares de trabajo, formatos y archivos genéricos, de tal manera que el reemplazo de personal en el desarrollo de las tareas, no impida la continuidad de las actividades de la empresa.

- Implementar procesos de rotación de personal en puestos de trabajo similares de la Unidad Administrativa, especialmente en aquellas tareas para las cuales solamente una persona hace la función.

- Mantener los registros de los sistemas de información al día de tal manera que la acumulación de trabajo y desactualización de datos no represente un riesgo para la ejecución del Plan de Continuidad.

- Solicitar a TI, respaldos periódicos de los archivos que se encuentran almacenados en sus estaciones de trabajo y que son necesarios para la prestación de servicios o procesamiento de las operaciones.

- Solicitar recuperación de información almacenada y verificar que esta haya sido almacenada correctamente.

4.9.4. Objetivos

Minimizar el daño al personal

- Minimizar el daño a los equipos e infraestructura
- Obtener un reporte de valoración de daños dentro de las cuatro primeras horas de interrupción
- Recuperar los sistemas y capacidades de procesamiento, almacenamiento y comunicación dentro del tiempo de recuperación objetivo establecido.

4.9.5. Procedimiento para reportar un evento potencial o real de desastre

Responsable: Personal vinculado directamente en el área de producción

Objetivo:
Reportar un evento potencial o real de desastre para tomar las acciones apropiadas y minimizar los daños al personal de la Organización y daños a los equipos, instalaciones o servicios.

EN CASO DE UN EVENTO QUE PONE EN SITUACIÓN DE RIESGO SU VIDA, DETENGA SUS ACTIVIDADES Y PÓNGASE A SALVO

1. Para reportar una situación de emergencia llame al 911. Reporte el tipo de emergencia, el nombre y dirección de la Institución: Cartopel – Parque Industrial
2. Notifique a cualquier miembro del Equipo de Continuidad sobre el evento de desastre.
3. Desaloje el edificio de acuerdo a los procedimientos establecidos.

4.9.6. Procedimiento para el Manejo del Evento

Responsable: Equipo de Continuidad

Objetivo: Decidir los detalles de implementación del Plan , coordinar toda la operación de manejo y recuperación, notificar al Grupo de Manejo de Crisis del tiempo de interrupción y

actividades de reparación estimadas; y, asistir en la resolución de los problemas que requiere el manejo del evento.

Antes del evento:

- Aprobar el Plan de Continuidad
- Asegurar que el Plan de Continuidad permanezca actualizado
- Coordinar y participar en eventos de formación para enfrentar emergencias
- Promover acciones para que el Equipo de Continuidad entienda su rol y responsabilidad dentro del Plan.
- Participar en pruebas del plan
- Asegurar que las pruebas y entrenamiento se ejecuten periódicamente

Durante el evento:

- Una vez que se ha ocurrido el evento, el Coordinador del Equipo de Continuidad, convoca a los miembros e informa del sitio y hora de reunión
- En caso de pérdida de personal clave, el Coordinador asigna a los empleados de más alto rango y que están en posición de dirigir el Plan de Continuidad para que asuman el rol que corresponda.
- El Coordinador Junto con los otros miembros del Equipo de Continuidad, conforma el grupo para Valoración de Daños y Pérdidas.
- El Coordinador, declara formalmente la emergencia e informa que el Plan de Continuidad se ha activado.
- El Coordinador, en base a la información obtenida por el equipo de valoración, se reúne con los otros miembros del Equipo de Continuidad y planifica las actividades para gestionar la contingencia.
- El Coordinador junto con los otros miembros del Equipo de Continuidad, determina la manera como se conducirá el Plan y que unidades administrativas deben trasladarse físicamente a otras oficinas así como la decisión de activar o no el Centro de Cómputo Alterno.
- El Coordinador monitorea y controla los procesos de recuperación de manera global.
- Los miembros del Equipo de Continuidad, monitorean y controlan los procesos de recuperación en lo que les compete.
- El Coordinador, facilita la adquisición de equipos, servicios y provisiones tomando en cuenta que se trata de una emergencia y que las formalidades pueden entorpecer las acciones de reparación y recuperación de las áreas afectadas.

- El Coordinador, informa permanentemente el Equipo de Manejo de Crisis, del avance de las actividades de recuperación.
- El Coordinador, disminuye las tensiones entre las/os empleados durante la contingencia.
- El Gerente de TI, en base al plan definido, coordina la activación del sitio alterno para que asuma las instrucciones, supervisa el desarrollo de los procedimientos, coordina, monitorea y controla la recuperación y reconstrucción del Centro de Cómputo Principal.

Al finalizar el evento:

- El Coordinador, verifica el estado de las actividades de reparación en el sitio del daño.
- Conjuntamente con los otros miembros del equipo de Continuidad, revisa y aprueba las actividades requeridas para volver a la normalidad, analiza las fechas probables de retorno, estrategias y prioridades.
- El Coordinador acuerda con el equipo de Manejo de crisis la fecha de retorno a las actividades normales.
- El Equipo de Continuidad desarrolla las actividades de retorno en lo que les corresponde.
- El responsable de TI, realiza las siguientes actividades para la desactivación del procedimiento de emergencia:

    - Verificar y comprobar que la infraestructura y servicios en el centro de Cómputo ha sido reparado y los servicios están disponibles.
    - Verificar y comprobar la restauración de la información, aplicativos, sistemas de operativos y servicios, en el Centro de Cómputo Principal.
    - Asegurar la accesibilidad a las aplicaciones y datos por parte de los usuarios.
    - Autoriza la desactivación del Centro Alterno
    - Monitorea el desempeño del Centro de Cómputo Principal
    - Verificar que los procesos de respaldo y recuperación se realizan con normalidad en el Centro de Cómputo luego del retorno.

- Los responsables de las Unidades Administrativas, realizan las siguientes actividades para la desactivación del procedimiento de emergencia:

    - Verificar y comprobar que la infraestructura y servicios requeridos para el desarrollo de las actividades de su departamento han sido reparadas, los servicios están disponibles y la operación es la adecuada.

  - Verificar y comprobar la restauración de la información y su integridad, en las aplicaciones que le competen a su área.
  - Asegurar la accesibilidad a las aplicaciones y datos por parte de los usuarios de su área.
- El Coordinador coordina y facilita los servicios y prestaciones necesarios para la desactivación del procedimiento y retorno a la normalidad.
- El Coordinador del Equipo de Continuidad, comunica que el plan se ha desactivado y el retorno a las actividades normales.

Cuando ha finalizado el Plan de Continuidad:

- El Coordinador dispone realizar la auditoría del resultado de las medidas de actuación previstas en el Plan.
- El Coordinador dispone la recolección de información de daños y pérdidas ocasionadas por el evento.
- El Equipo de Continuidad analiza los informes, evalúa los resultados y propone ajustes al Plan de ser necesario.
- El Coordinador presenta el informe respectivo al Equipo de Manejo de Crisis.

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida.

4.9.7. Valoración de Daños y Rescate

Responsables: *Gerente Administrativo, Superintendente de Producción, Jefe de Seguridad, Gerente de (TI).*

Objetivo: *Valorar los daños e impacto causado por el evento, proponer acciones orientadas a proteger al personal, asegurar y rescatar los activos y reparar los daños provocados por el evento.*

Antes del evento:

- Son entrenados en la preparación para enfrentar emergencias.
- Entienden su rol y responsabilidad dentro del Plan.
- Trabajan muy de cerca con el Equipo de Continuidad para reducir las posibilidades de desastres en el Edificio y en el Centro de Cómputo.
- Participan en pruebas del plan cuando son requeridos.
- Elaboran una guía para revisar y valorar posibles daños.

Después del evento:

- Valorar el daño de la infraestructura y servicios básicos así como del centro de cómputo en el menor tiempo posible y estimar el tiempo y requerimientos de la recuperación. Utilizar la lista como una guía para revisar y valorar los daños.
- Una vez realizada la valoración, debe tener respuestas para las siguientes preguntas:
  - Es el área segura para que los empleados trabajen y los clientes puedan ingresar sin ningún riesgo?
  - Pueden trabajar los equipos de TI? Qué porcentaje de capacidad normal debería esperarse?
  - Que debe hacerse para recuperar las capacidades y prestaciones normales?
  - Qué tiempo tomará reemplazar o reparar los equipos dañados para volver a la normalidad?
- Basado en la valoración de daños, determinar el tiempo estimado de recuperación en el marco de los siguientes lineamientos:

Nivel de daño	Descripción
Nivel I Mínimo	Daño no estructural aislado; costo de reparación < 10% del valor de mercado del edificio y/o equipamiento Daño mínimo a las facilidades y el equipo. El tiempo para completar la reparación se estima entre 2 y 4 días.
Nivel II Moderado	Daño considerable no estructural y daños estructurales ligeros; costo de reparación menor al 25% del valor del mercado Daño moderado. Se estima la reparación entre 5 y 7 días.
Nivel III Extenso	Daño estructural considerable y daño no estructural excesivo; costo de reparación < al 50% del valor del mercado Daño extenso. Se estima que la reparación tomará más de una semana laborable.

Grafico No. 20: “Valoración de daños y rescate”

- Valorar la necesidad de seguridad física tal como guardias de seguridad
- Determinar la accesibilidad al edifico y oficinas.
- Notificar al Equipo de Continuidad acerca de la valoración, tiempos de recuperación estimados, requerimientos de seguridad física y equipos recuperables.
- Facilitar el ingreso de personal externo y eliminar el riesgo de potenciales actividades de vandalismo.
- Coordinar con vendedores y proveedores la restauración, reparación o reemplazo de equipos de procesamiento, almacenamiento o comunicación.
- Proveer soporte en la limpieza del sitio y reparación del Centro de Cómputo y áreas afectadas.

Importante: Bajo ninguna circunstancia puede hacer pública la valoración e información recogida.

4.9.8. Seguridad Física

Responsable: Jefe de Seguridad

Objetivo: Prestar seguridad física en el sitio del desastre y verificar la seguridad del sitio alterno, actuar en coordinación con el personal de servicios de emergencia.

Antes del evento:

- Entrenado en la preparación para enfrentar emergencias
- Entiende su rol y responsabilidad dentro del Plan.
- Trabaja muy de cerca con el Equipo de Continuidad para garantizar seguridad física.
- Participar en pruebas del plan cuando son requeridos.

Después del evento:

- Establece seguridad física en las instalaciones, restringiendo el acceso a las áreas dañadas únicamente para aquellos que requieren realizar trabajos de reparación o investigación: investigadores, contratistas, etc.
- Coordina la autorización de acceso al personal
- Dependiendo de la extensión del daño coordina con el personal de policía y emergencia los accesos.
- Dependiendo del evento provee de guardias de seguridad a las áreas
- Coordina los horarios y salidas de equipos, archivos o reportes.

- Asiste a los investigadores y aseguradores en el sitio del daño.

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida.

4.9.9. Administración

Responsable: *Gerente Administrativo*

Objetivo: Proveer soporte administrativo a todo el personal que conforma el Equipo de Continuidad incluyendo actividades de adquisiciones viajes, adquisición y compra de teléfonos y otras funciones que no proveen los demás equipos.

Antes del evento:

- Entrenado en la preparación para enfrentar emergencias
- Entiende su rol y responsabilidad dentro del Plan.
- Trabaja muy de cerca con el Equipo de Continuidad para garantizar soporte administrativo.
- Participar en pruebas del plan cuando son requeridos.

Después del evento:

- Prepara, coordina y obtiene las aprobaciones apropiadas para los requerimientos de adquisiciones.
- Coordina la entrega de los bienes adquiridos.
- Procesa los requerimientos para pago en todo lo relacionado al proceso de recuperación.
- Hace arreglos de transportes, movilización y hospedaje.
- Provee medios de comunicación emergentes.
- Hace arreglos para proveer servicios de secretaria, archivo u otros requeridos por el Equipo de Continuidad.
- Realiza la adquisición e instalación de quipos y servicios de telefonía emergentes y que son requeridos.
- Documenta y agilita los trámites con las aseguradoras

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida**.**

4.9.10. Infraestructura del Centro de Cómputo

Responsable: Jefe de Producción, Gerente Administrativo y Jefe de Informática

Objetivo: Planear, diseñar, programar y verificar la correcta activación del Centro Alterno y en el marco de los tiempos establecidos, así como el restablecimiento de estos servicios en el Centro de Cómputo Principal cuando este ha sido reparado.

Antes del evento:

- Entrenado en la preparación para enfrentar emergencias
- Entiende su rol y responsabilidad dentro del Plan.
- Trabaja muy de cerca con el Equipo de Continuidad para garantizar la correcta activación y desactivación del Centro Alterno.
- Participar en pruebas del plan cuando son requeridos.
- Verificar periódicamente que los sistemas operativos, información y aplicativos son respaldados adecuadamente y su recuperación está garantizada.
- Verificar periódicamente que los servicios de proveedores cuentan con alternativas para responder en momentos de emergencia.

Después del evento:

- Participa en la valoración de daños y hace propuestas para el desarrollo de actividades de restauración y recuperación
- Verifica e inspecciona la disponibilidad de facilidades en el Centro Alterno y ejecuta la activación.
- Aplica el plan de activación del Centro Alterno, levantando los sistemas operativos, software especializado, bases de datos y aplicativos.
- Prueba y verifica que la habilitación de aplicaciones, servicios, base de datos y demás componentes fue completa y exitosa.
- Mantiene registro de los equipos y servicios de TI y de su estado de afectación en el Centro de Cómputo Principal.
- Asiste en el desalojo de las áreas afectadas en el Centro de Cómputo Principal y retiro de los equipos o dispositivos que deben ser reparados o reemplazados.
- Coordina las adquisiciones o reparación de equipamiento y servicios necesarios para la recuperación del Centro de Cómputo Principal y verifica el funcionamiento apropiado.
- Propone procedimientos para retorno a las actividades normales.

- Ejecuta las actividades de retorno, desactivando el Centro de Cómputo Alterno y activando el centro de Cómputo Principal.

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida.

4.9.11. Servicios de Comunicaciones

Responsable: Jefe de Comunicaciones y Jefe de (TI).

Objetivo: Planear, diseñar, programar y verificar la correcta activación de las Comunicaciones tanto internas como externas en el Centro Alterno y en el marco de los tiempos establecidos, así como el restablecimiento de dichos servicios en el Centro de Cómputo Principal cuando este ha sido reparado.

Antes del evento:

- Entrenado en la preparación para enfrentar emergencias
- Entiende su rol y responsabilidad dentro del Plan.
- Trabaja muy de cerca con el Equipo de Continuidad para garantizar la correcta activación y desactivación de las comunicaciones tanto internas como externas en el Centro Alterno.
- Participar en pruebas del plan cuando son requeridos.
- Verificar periódicamente que los procesos de activación y desactivación de servicios de comunicación son válidos.
- Verificar periódicamente que los servicios de proveedores cuentan con alternativas para responder en momentos de emergencia.

Después del evento:

- Participa en la valoración de daños y hace propuestas para el desarrollo de actividades de restauración y recuperación
- Verifica e inspecciona la disponibilidad de los servicios de comunicación tanto internos como externos.
- Aplica el plan de activación del Centro Alterno, levantando los sistemas de comunicación.
- Prueba y verifica que la habilitación de los servicios fue completa y exitosa.
- Mantiene registro de los elementos de red y de su estado de afectación en el Centro de Cómputo Principal.

- Asiste en el desalojo de las áreas afectadas en el Centro de Cómputo Principal y retiro de los equipos o dispositivos de red que deben ser reparados o reemplazados.
- Coordina las adquisiciones o reparación de equipamiento y servicios necesarios para que los servicios de comunicación funcionen apropiadamente en el Centro de Cómputo Principal que está siendo reparado.
- Propone procedimientos para retorno a las actividades normales.
- Ejecuta las actividades de retorno, desactivando el sistema de comunicaciones desde el Centro de Cómputo Alterno y activándolo en el centro de Cómputo Principal.
- Prueba y verifica la operación del sistema de comunicaciones una vez que se han levantado los servicios y se ha desactivado el proceso.

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida.

4.9.12. Soporte a Usuarios

Responsable: Jefe de Producción

Objetivo: Planear, diseñar, programar y verificar la correcta activación de las estaciones de trabajo de los usuarios de las unidades administrativas movilizadas y de planta en el marco de los tiempos establecidos, así como el restablecimiento de las áreas físicas de los usuarios han sido reparadas.

Antes del evento:

- Entrenado en la preparación para enfrentar emergencias
- Entiende su rol y responsabilidad dentro del Plan.
- Trabaja muy de cerca con el Equipo de Continuidad para garantizar la correcta instalación de las estaciones de trabajo para los usuarios eventualmente movilizados.
- Participa en pruebas del plan cuando son requeridos.
- Verifica periódicamente que los procesos de respaldo y recuperación de información de las estaciones de trabajo sean válidos.
- Verifica periódicamente que los servicios de proveedores cuentan con alternativas para responder en momentos de emergencia.

Después del evento:

- Participa en la valoración de daños y hace propuestas para el desarrollo de actividades de restauración y recuperación

- Verifica e inspecciona la disponibilidad de las estaciones de trabajo y su conectividad en las unidades administrativas afectadas.
- Mantiene registro de las estaciones de trabajo y puntos de conexión afectados.
- Asiste en el desalojo de las áreas afectadas y retiro de los equipos o dispositivos de red que deben ser reparados o reemplazados.
- En el marco de la estrategia establecida, coordina con los proveedores el reemplazo o reparación de equipamiento y servicios necesarios para que las estaciones de trabajo funcionen adecuadamente.
- Instala aplicativos e información, de acuerdo al perfil de los usuarios, en las estaciones de trabajo que fueron reemplazadas o reparadas.
- Presta soporte a los usuarios para su operación.

Importante: Bajo ninguna circunstancia puede hacer pública la información recogida.

4.10. ADMINISTRACIÓN DEL PLAN DE CONTINUIDAD

Los procedimientos descritos en este párrafo tienen como objetivo mantener un estado actualizado y consistente.

El propósito de este capítulo es identificar las acciones que deben realizarse para que Cartopel mantenga el Plan de Continuidad en permanente vigencia.

4.10.1. Acciones requeridas

Las principales tareas que debe asumir el Equipo de Continuidad son:

- Distribución y difusión del Plan
- Mantenimiento del Análisis de Impacto y Gestión del Riesgo Operativo asociado a eventos de desastre.
- Fortalecimiento de la Cultura Institucional para la prevención de desastres.
- Pruebas
- Evaluaciones
- Revisiones, cambios y actualizaciones.

4.10.2. Distribución y Difusión del Plan

El Coordinador es responsable de la distribución autorizada del plan. Como se trata de un documento confidencial requiere una lista de distribución autorizada en la que consten los nombres de los directivos de las unidades administrativas, en el caso de archivos digitales se instalará en el servidor apropiado con acceso restringido.

La entrega de las copias se realiza formalmente y requiere la firma del receptor reconociendo la confidencialidad del documento; y, la obligación de leer y conocer el contenido de cada una de las secciones; y, las funciones específicas que le corresponden y que están definidas en este documento.

La entrega de nuevas versiones requerirá de la recolección de las versiones anteriores como paso previo, a fin de mantener control de las versiones.

Son personas autorizadas:

- Los integrantes del Equipo de Continuidad
- Los responsables de las Unidades Administrativas
- Los responsables de equipos de trabajo internos de la Gerencia de TI

El Coordinador del Equipo de Continuidad organiza y participar en eventos de capacitación y difusión del plan para los miembros del equipo y responsables de unidades administrativas.

Los responsables de las unidades administrativas organizan y participan al interior de su unidad en eventos de capacitación y difusión del plan.

4.10.3. Mantenimiento del Plan

Debido a que los condicionantes y estrategias del negocio pueden variar, también los requerimientos del Plan de Continuidad pueden hacerlo. Se establecen las siguientes recomendaciones de actualización:

Fase	Recomendación de actualización
Fase I: Políticas del Plan,	El impacto de la estrategia de la empresa se revisa al menos una vez al año, puede coincidir o ser parte de los procesos de

Contexto de la Empresa y Enfoque	planeación de la estrategia de la empresa. Además se revisa en las siguientes circunstancias: o Cambio de estrategia de la empresa o Reestructuraciones, expansiones o contracciones de la empresa o Introducción de nuevos productos en el mercado
Fase II: Analizar Riesgos e Impacto en la empresa	Se revisa anualmente y con más frecuencia en las siguientes circunstancias: o Cuando un cambio en el negocio es particularmente agresivo o Cuando hay cambios significativos en el proceso interno, ubicaciones geográficas o tecnología. o Cuando hay un cambio significativo en el ambiente externo, por ejemplo: mercado o regulaciones.
Fase III: Analizar Estrategia y Respuesta	**ESTRATEGIA** Se revisa anualmente y con más frecuencia en las siguientes circunstancias: o Cambios en la criticidad y procesos de la empresa o Cambios significativos en Tecnología, apetito de riesgo, ubicaciones geográficas, staff. proveedores, leyes o regulaciones **PLAN** Revisiones de información de detalle se realizarán trimestralmente, otra información se revisará como resultado de las pruebas. Los siguientes elementos pueden modificar el plan en cualquier momento: o Un cambio significativo en tecnología o comunicaciones o Un cambio importante en algún segmento del negocio o Un cambio del staff o Un cambio de proveedor o Un cambio en la solución del proveedor

Grafico No. 21: “Mantenimiento del Plan”

4.10.4. Pruebas del Plan

El coordinador del Plan y los integrantes del Equipo de Continuidad, son responsable de que se realicen pruebas, sean parciales o totales, y de manera periódica para asegurar de la viabilidad del plan.

Los objetivos de la Prueba son:

- Detectar falencias en los procedimientos
- Determinar el estado de prontitud y habilidades de los miembros del equipo.
- Determinar el grado de disponibilidad de los equipos y facilidades del sitio alterno.
- Determinar si el Plan requiere actualizaciones o modificaciones
- Asegurar que los tiempos de recuperación objetivos son aceptables para los usuarios.

Aspectos que deben considerarse para realizar las pruebas:

- Objetivo y Alcance
- Restricciones y Consideraciones
- Requerimientos de Personal
- Requerimientos de Equipo y material
- Fecha Propuesta
- Duración
- Presupuesto y Cronograma
- Revisión de la ejecución

4.10.5. Medición y Evaluación de las Pruebas

El Equipo de Continuidad es responsable de la revisión y análisis de los resultados de la prueba. Conforma el equipo encargado de registrar las acciones que se llevan a cabo durante la prueba y tiene las siguientes responsabilidades:

- Familiarizarse con el plan
- Entender los objetivos de la prueba
- Organizarse para monitorear y observar las actividades
- Registrar las actividades que realizan los diferentes actores en base a los procedimientos definidos para ejecutar la prueba

- Revisar los resultados de la prueba desde el punto de vista del personal de TI y de los usuarios.
- Documentar para informar de las debilidades y fortalezas encontradas
- Planificar la siguiente prueba, de ser necesario.

El coordinador convoca a una reunión a los Equipos de Trabajo, revisan los resultados obtenidos, discuten sobre la solución a los problemas encontrados y planifican la siguiente prueba de ser necesario.

El Coordinador preside las reuniones y coordina que se realicen los cambios acordados en el Plan de Continuidad.

CAPITULO V

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES Y RECOMENDACIONES

5.1.1 CONTRA LA ACCIÓN DE VIRUS

Conclusión:

Se ha constatado que Cartopel trabaja con el antivirus Karpensky en todas las estaciones así como en el servidor, lo que no garantiza la seguridad en la información ni de los sistemas, por cuanto existen varios virus que pueden ser propagados sin ser detectados en toda la red.

Recomendación:

Según lo mostrado en la situación actual en la sección de esquema de antivirus, es necesario estandarizar el software de antivirus en todas las estaciones de trabajo y servidores. Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, debido a que éstos tienen variaciones en sus tablas de definiciones de virus, además es más difícil que un virus se propague por la red debido a la diversificación de productos que puedan detectarlos y así podríamos reducir la probabilidad de que un virus que no esté en la lista de actualización, se filtre en toda la red.

Es necesario implementar un procedimiento para las actualizaciones automáticas de las definiciones de virus, tanto para Norton como para Macfee. Esta labor la debe realizar el administrador de red, cuidando que se ejecute en horas en que no se degrade el performance del tráfico de red.

5.1.2. CONTRA ACCESOS NO AUTORIZADOS

Conclusión:

Si bien es cierto la empresa en algunas áreas presenta sistemas de seguridad física e informática para evitar accesos no autorizados, existen otras secciones que están expuestas a mal uso ya sea por negligencia y por qué no decirlo por “criminalidad”.

Recomendación:

Frente a este riesgo potencial, es necesario implementar lo siguiente:

- El servidor de archivos no debe ser accesible físicamente a cualquier persona.
- Es conveniente que exista un espacio físico donde se ubique el servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su

funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.

- En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

5.1.3. CONTRA FALLAS EN LOS EQUIPOS

Conclusión:

Existen gran desconocimiento en cuanto al manejo de los equipos (uso y mantenimiento) por parte algunos funcionarios que forman parte de la empresa y que se encuentran vinculados en áreas estratégicas del proceso de producción.

No obstante el departamento de informática realiza periódicamente el mantenimiento y limpieza de hardware pero por motivos de tiempo no abastecen toda la planta.

Recomendación:

- La primera opción será designar a uno o más empleados a que dediquen un tiempo para el aprendizaje y formación, mediante la toma de un curso, para que ellos sean los encargados en brindar mantenimiento preventivo y correctivo a los equipos que posee la empresa.
- Como otra opción sugerimos el contratar los servicios de una empresa que de forma periódica realice mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.
- Sea la decisión que se escoja se sugiere que como mínimo se realice por lo menos una vez al año y llevar un control, de la vida útil de los diferentes dispositivos.
- Para evitar el caos que provocaría una avería en el servidor de archivos, o en uno de sus discos duros, plantéese la utilización de un cluster.
- Un sistema de alimentación sin interrupciones (UPS) es hoy en día imprescindible, al menos para el servidor de archivos, el servidor proxy y el HUB/Switch.
- Al llevar un control de lo instalado mediante las listas de software se recomienda que todo nuevo software que se piense instalar sea probado en un computador que posea el software estándar para las actividades de la empresa con la finalidad de confirmar que este nuevo software no afectara a los otros ya instalados.

5.1.4. CONTRA OTROS POSIBLES SINIESTROS

Conclusión: En función de los antecedentes expuestos, se puede confirmar que existen varios tipos de riesgos que atentan el normal desenvolvimiento de las actividades de

producción de la Empresa Cartopel; en tal sentido es imprescindible que a futuro la empresa una vez que cuenta con los resultados del estudio del Plan de Contingencia, inicie el proceso respectivo para su aprobación y posterior implementación para que de esta manera Cartopel y el personal que la conforma se encuentre preparado para darle frente a un inesperado siniestro que pueda acarrear demoras, retrasos y como consecuencia pérdidas irreversibles de carácter humano, económico e informático, para el efecto es necesario conocer las acciones específicas a seguir para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática.

Recomendación:

Para el efecto considero necesario recalcar 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 (extintores, 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.

Considero que frente a los incidentes y accidentes repentinos la protección de la Integridad del personal es prioritaria, sin embargo, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), y para prevenir pérdidas mayores considero que debe 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, para salvar los equipos señalados en las actividades previas al desastre.

Y por último un aspecto importante es que el personal tome conciencia de que los diversos siniestros ya sean naturales o inducidos y que tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, es necesario eventualmente implementar simulacros y charlas ante los posibles siniestros que pudiesen ocurrir en la empresa.

BIBLIOGRAFÍA

- **INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – DIRECCIÓN NACIONAL DEL SEGURO GENERAL DE RIESGOS DEL TRABAJO.-** Seguro General de Riesgos del Trabajo Normativas, Octubre 2008.

- **CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES.-** Ley de Defensa Contra Incendios – Reglamentos y Legislación Conexa, Actualizada a marzo de 2011.

PÁGINAS WEB

- http://definicion.de/plan-de-contingencia/.- **COPYRIGHT © 2008-2011.–** DEFINICIÓN DEL PLAN DE CONTINGENCIA,
- http://www.ferratermora.org/ency_concepto_ad_contingencia.html.- **COPYRIGHT©2002 JOSEP FERRATER MORA FOUNDATION.-** CONTINGENCIA
- es.wikipedia.org/wiki/Plan_de_Contingencia.- **WIKIPEDIA ENCICLOPEDIA LIBRE JIMMY WALES FUNDADOR.-** PLAN DE CONTINGENCIAS,
- www.binasss.sa.cr/poblacion/desastres.htm.- **PROGRAMA EDUCATIVO PARA EMERGENCIAS- P.E.E.M.E.P-** COMPENDIO GENERAL SOBRE DESASTRES,
- http://www.s21sec.com/servicios.aspx?sec=47&apr=51.- **S21 SEC-COMPROMETIDOS CON LA SEGURIDAD.-** PLANES DE CONTINGENCIA INFORMATICA,
- http://www.segu-info.com.ar/politicas/contingencia.htm.- **Copyright © Cristian Borghello 2000 - 2009 SEGU INFO – SEGURIDAD DE LA INFORMACION,** PLAN DE CONTINGENCIA,

Glosario

Entidad / Institución: Una compañía, firma, empresa o asociación, u otra entidad legal o parte de ella, sea o no incorporada, pública o privada que tiene sus propias funciones y administración.

Proceso: Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente.

Proceso Crítico: aquellos cuya interrupción puede impedir el normal funcionamiento de la Entidad, la consecución de los objetivos y provocar pérdidas financieras.

Unidad Administrativa: Dirección, Departamento o Gerencia representada en el Organigrama de la Entidad, tiene a cargo un conjunto de procesos o subprocesos especializados que generan productos y/o servicios para el cliente o para otras Unidades.

Desastre: situación catastrófica en la cual las pautas de la vida cotidiana han sido interrumpidas súbitamente y afectan a gran número de personas y de activos.

Crisis: Una situación que pone a juicio los valores de una empresa ante la opinión pública.

Accidente: Suceso casual e involuntario que altera el orden regular de las cosas.

Evento de Riesgo: suceso que al producirse tiene un impacto negativo sobre los Objetivos de la Institución.

Impacto: Es el nivel de afectación que tienen los objetivos o procesos institucionales debido a la presencia de un evento de riesgo.

Probabilidad: Es la posibilidad de ocurrencia de un evento especifico o resultado, medido por la relación de eventos específicos o resultados ocurridos anteriormente sobre el número total de posibles eventos o resultados.

Contingencia: situación de alteración del funcionamiento normal de una o más actividades de negocio, debido a un accidente, desastre o crisis.

Plan de Contingencia: conjunto de medidas encaminadas a restaurar el funcionamiento normal de una o más actividades, tras la alteración producida por un accidente, desastre o crisis.

Tiempo de recuperación objetivo: Cantidad de tiempo adecuada de recuperación de los sistemas informáticos de la Institución después de que ocurre un accidente, desastre o crisis.

Equipo de Continuidad: Grupo de trabajo designado por los Directivos del Cartopel para realizar acciones antes durante y después de un evento de riesgo que atenta la capacidad operacional y la prestación de servicios de la Institución.

GCM (Gestión de la Continuidad del Negocio): Es un proceso integral que identifica los impactos potenciales que amenazan a la Institución y provee un marco para la construcción de una estrategia de contingencia cuya capacidad de respuesta salvaguarde los intereses de los accionistas, reputación, marca y actividades de generación de valor.

PRD/CN (Plan de Recuperación de Desastres y Continuidad del Negocio): Es el conjunto de acciones y recursos de que dispone la Institución para recuperar y mantener los procesos, operaciones y funciones críticas a pesar de circunstancias o situaciones adversas. Comprende el planeamiento y los procedimientos previos, durante y posteriores al evento.

ANEXOS

ANEXO 1

CRONOGRAMA DE TESIS

ACTIVIDAD	AGOSTO		SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.- Presentación y aprobación del tema del anteproyecto	22-27		cumplido											
2.- Identificación y delimitación del problema		29-03	cumplido											
3.- Desarrollo del Marco teórico.			05-10	cumplido										
4.- Recopilar organizar, clasificar, comparar e interpretar la información.				12 sep al 22 oct						cumplido				
5.- Extracción de conclusiones, redacción final y revision del Director de tesis									23 -30 oct	cumplido				
6.- Entrega de esquema de tesis (3 ejemplares)										31 oct cumplido				
7.- Sustentación de tesis											? 05-30 ?			

Grafico No. 22: “Cronograma de Tesis”

ANEXO 2

La empresa Cartopel está constituida por diferentes departamentos los cuales fusionan conjuntamente entre ellos para así tener éxito en las metas propuestas por la gerencia a continuación tenemos el diagrama del orgánico funcional de la empresa:

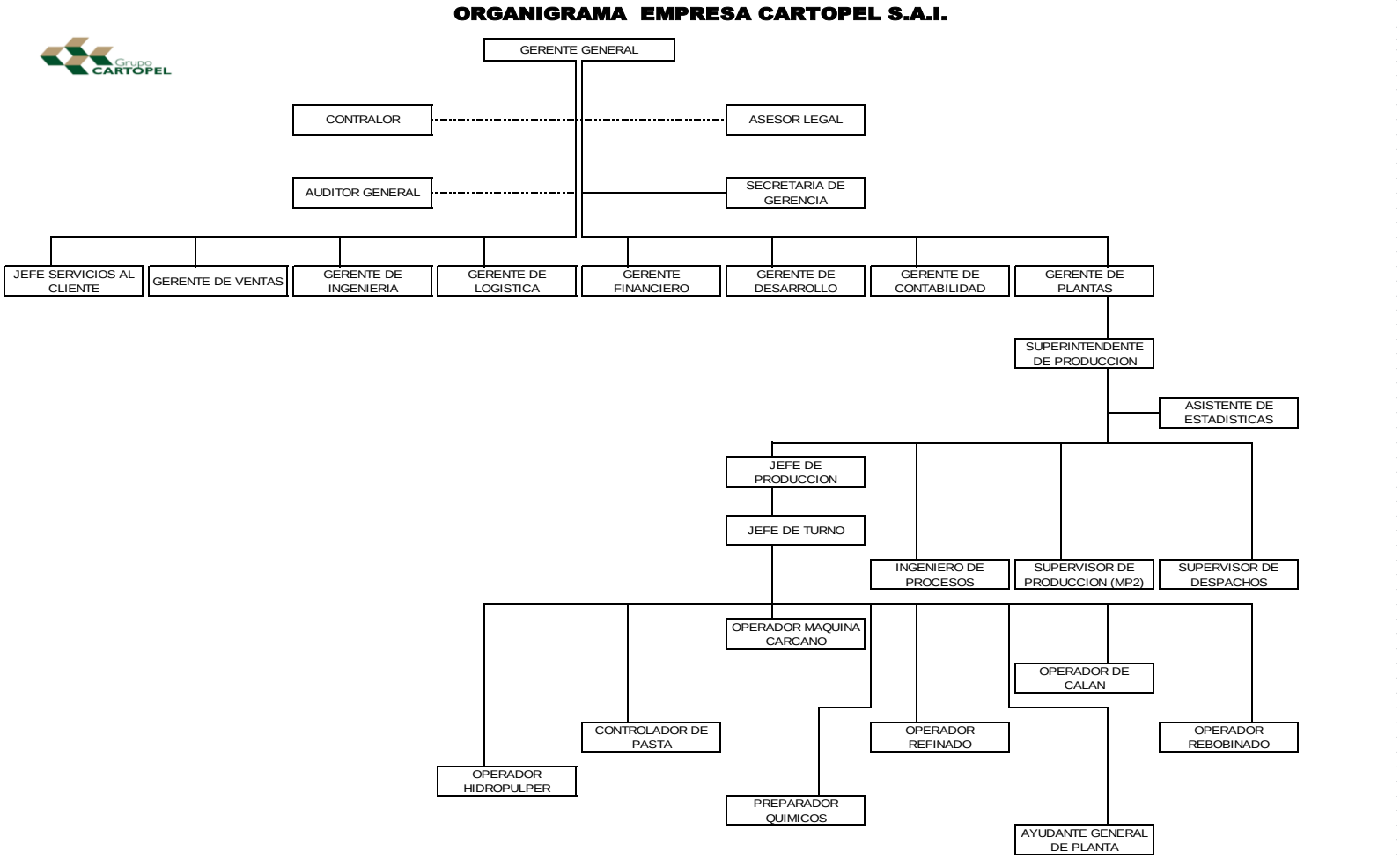

Grafico No. 23: “Organigrama de la Empresa Cartopel S.A.I.”

ANEXO 3

ENTREVISTA

La entrevista fue aplicada a los Jefes Departamentales vinculados directamente con el área de Producción, sus datos no son posibles tabularles por cuanto son preguntas abiertas, a continuación detallo sus resultados:

1. Existe un Plan de Contingencias contra desastres informáticos para el área de producción de la Empresa?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
NO EXISTE	DESCONOCE	NO EXISTE UN PLAN PARA ESTA ÁREA

2. Con qué servidores contamos en la empresa?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
DESCONOCE	DESCONOCE	SERVIDOR DE DATOS SERVIDOR DE APLICACIONES SERVIDOR WEB

3. Qué sistemas y aplicaciones se maneja en el área de producción?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
COMET 2100 – Control de Procesos SISTEMA NAF – Controlador de Driver CONNET – Control de Inventarios, de Producción, Registro de Asistencias	CONNET – Control de Inventarios, de Producción, Registro de Asistencias INTEGRA – Control de Inventarios	COMET 2100 – Control de Procesos INTEGRA – Control de Inventarios CORPLAN

4. Ha existido algún incidente mayor en estas áreas?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
SI, se han quemado módulos de datos por variación de voltaje. Falta de ventilación Daños en Aire Acondicionado	No muy graves	Daño en sistema COMET 2100 – Control de Procesos

5. Quienes son los responsables directos de levantar los servicios en caso de un incidente?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
Departamento de Sistemas Departamento Eléctrico	Departamento de Sistemas	Departamento de Tecnologías Informáticas

6. Cuán importantes son los sistemas informáticos dentro de esta área?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
Muy importante	Alta no se puede trabajar sin estos sistemas	Muy importantes

7. Cree usted que es necesario contar con un Plan de Contingencias contra desastres para ésta área?

Ing. José Guerrero JEFE DE PROCESO	Ing. Wilmer López JEFE DE DESPACHOS	Ing. Fabián Bustamante GERENTE INFORMÁTICO
Si debería existir	Efectivamente	Si muy importante

8. Qué tiempo máximo cree usted que puede estar sin servicio informático ésta área?

Ing. José Guerrero **JEFE DE PROCESO**	**Ing. Wilmer López** **JEFE DE DESPACHOS**	**Ing. Fabián Bustamante** **GERENTE INFORMÁTICO**
El sistema COMET 2100 – Control de Procesos, dependiendo del incidente El SISTEMA NAF – Controlador de Driver podemos prescindir 1 a 2 días El Sistema CONNET – Control de Inventarios, de Producción, Registro de Asistencias, podemos prescindir 1 a 2 días	Los dos sistemas CONNET – Control de Inventarios, de Producción, Registro de Asistencias e INTEGRA – Control de Inventarios, un período máximo de 8 horas.	Los sistemas COMET 2100 – Control de Procesos, INTEGRA – Control de Inventarios y CORPLAN, máximo 4 horas dependiendo de la criticidad.

De la entrevista realizada a los Jefes Departamentales que se encuentran vinculados directamente con el departamento de producción, puedo determinar que es imprescindible a corto plazo implementar un plan de Contingencias para optimizar el plan de acción, mejorar las actividades que podrían causar dificultad durante un siniestro y/o causar una pérdida o retraso en el normal desenvolvimiento del proceso de producción; así mismo reforzar los elementos que funcionaran adecuadamente para minimizar los riesgos y pérdida durante un siniestro.

El resultado de las entrevistas como se puede observar poco o nada conocen de un plan de contingencias, o lo relacionado al área de sistemas es por eso que al implementar un plan de contingencias existe una etapa en la que se capacitaría sobre este tema no solo a las jefaturas sino a todo el personal de la empresa.

ANEXO 4

INVENTARIO DE HARDWARE	INVENTARIO DE SOFTWARE
PISO MÁQUINA	**PISO MÁQUINA**
Oficina del Jefe de Turno – Producción	**Oficina del Jefe de Turno - Producción**
1 CPU IBM	Windows XP (Sistema Operativo)
1 monitor 14” HP	Connet (Sistema control de personal)
	Karpensky (antivirus)
Oficina de Jefe de Producción	**Oficina de Jefe de Producción**
1 CPU HP	Windows XP (sistema operativo)
1 monitor de 17” Samsung	Connet (Sistema control de personal)
	Karpensky (antivirus)
Sala de Monitoreo	
2 CPU HP	**Sala de Monitoreo**
4 monitores LG 20”	Comet 2100 (sistema de control de peso y humedad)
1 impresora HP	Scada (Sistema de control de subestación y calderas)
	Sistema de Control de drives
	Karpensky (antivirus)
Sala de Control	**Sala de Control**
2 CPU HP	Comet 2100 (sistema de control de peso y humedad)
2 monitores 14” HP	Karpensky (antivirus)
1 impresora Samsung	
Control de Calidad	**Control de Calidad**
1 CPU HP	Windows XP (Sistema Operativo)
1 monitor de 17”	Connet (Sistema control de personal)
	Karpensky (antivirus)
PISO INFERIOR	**PISO INFERIOR**
Despachos	**Despachos**
2 CPU HP	Connet (Sistema control de personal)
1 monitor HP 14”	FTP (Reporte de Envíos)
1 monitor HP 17”	Integra Web (Autorización de camiones)
1 impresora EPSON	