


	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

INTRODUCCION

En el procedimiento y plan de contingencia informática se definen los objetivos, alcance, responsable, factores críticos, definiciones, aspectos generales de seguridad, las fases del plan de contingencia teniendo en cuenta análisis de riesgos, acciones ante la probabilidad de que ocurra un riesgo, definición del equipo de trabajo, identificación de eventos entre otros.

El Procedimiento y plan de contingencia informática permitirá mantener la continuidad de los sistemas de información frente a eventos críticos, de **SI LOGISTICA** y minimizará el impacto negativo sobre la misma, sus recursos y usuarios.

Este plan es parte integral de las políticas informáticas de **SI LOGISTICA** que servirá para evitar interrupciones, para estar preparado contra fallas potenciales y para guiar hacia una solución oportuna en la restauración del servicio.


Es importante resaltar la importancia de garantizar en todo momento la continuidad de los Sistemas de Información y de este modo aumentar la confianza de los usuarios en las transacciones y procesos que realizan a través de ellos. Este instrumento se ha diseñado en este sentido, para dar respuesta oportuna, adecuada y coordinada a situaciones de emergencia causadas por fenómenos destructivos de origen natural o humano.

OBJETIVO GENERAL

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información para **SI LOGISTICA**, Implementando un Plan de Contingencia Informático, que contenga los procedimientos e instructivos necesarios para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia. Así como minimizar el impacto que dichos daños pudieran causar.

OBJETIVOS ESPECÍFICOS

- ✓ Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de la **SI LOGISTICA**
- ✓ Definir y aplicar medidas para prevenir los riesgos; detectar y corregir las desviaciones que se presentan en **SI LOGISTICA**, y que puedan afectar el logro de sus objetivos

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

- ✓ Proveer una solución para mantener los procedimientos administrativos, sistemas de información y equipos de cómputo fundamentales de **SI LOGISTICA**, funcionando correctamente
- ✓ Conservar la memoria documental del área operativa y administrativa para mantener la prestación del servicio en niveles aceptables.
- ✓ Reducir las consecuencias y evitar una posible pérdida de información relacionada con un evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.
- ✓ Establecer mecanismos y procedimientos para proporcionar confidencialidad, integridad y disponibilidad de la información.
- ✓ Estimular la creación de una cultura de seguridad en Informática entre los miembros de la Institución
- ✓ Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.
- ✓ Continuar con las funciones de las diferentes áreas de **SI LOGISTICA**, que se haya visto afectadas por una situación adversa.
- ✓ Prevenir o minimizar el daño permanente a los recursos informáticos

ALCANCE

Aplica para los equipos de cómputo, sistemas de información, telecomunicaciones y tecnología de **SI LOGISTICA**


RESPONSABLES

Asistente administrativa y soporte tecnología son las la personas responsables de que este plan se cumpla y de asegurar el entrenamiento del personal para el conocimiento de este procedimiento.

DEFINICIONES

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto, hojas de cálculo, imágenes, vídeo, etc.

Equipos de cómputo: Elementos o dispositivos de hardware, software, redes y telecomunicaciones interconectados que son utilizados para lleva a cabo las actividades operativas sistematizadas de la compañía.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION: 1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

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

Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación.

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

Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de un computador o causar la difusión no autorizada de información confiada en un servidor. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

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

Plan de contingencia: Estrategia planificada con una serie de procedimientos que faciliten u orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la Institución ante la eventualidad de todo lo que se pueda paralizar, ya sea de forma parcial o total.

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


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

Sistema de Información: Organización sistemática para almacenar los datos de una organización y ponerlos a disposición de su personal

ASPECTOS GENERALES DE LA SEGURIDAD DE TECNOLOGIA INFORMATICA

SEGURIDAD FISICA:

<p>Garantiza la integridad de los activos lógicos y materiales de un sistema de información y de su infraestructura.</p>
--

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Desde el edificio en donde se encuentran ubicados los dispositivos el enfoque debe ser a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico del entorno.

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o para aminorar las consecuencias que de él se puedan derivar. Algunos aspectos a considerar son:

- ✓ Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- ✓ Potencia eléctrica.
- ✓ Sistemas contra Incendios.
- ✓ Control de accesos.
- ✓ Selección de personal.
- ✓ Medidas de protección.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

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.

Amenazas ocasionadas por el hombre:

Los componentes de la infraestructura tecnológica son posesiones valiosas de la Compañía y pueden estar expuestas.


Es frecuente la utilización de los equipos de cómputo de la compañía para realizar labores de cada cargo y de esta manera, utilicen tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. El software, es una propiedad muy fácilmente de sustraer y los discos o cintas son fácilmente transportados y llevados fuera del recinto.

Recomendaciones:

Todos los equipos que componen la infraestructura tecnología de la compañía deben estar instalados de manera no fácil de sustraer o acceder.

Su posicionamiento y ubicación se debe registrar y auditar de manera frecuente.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

El uso que los funcionarios de la compañía dan a los diferentes componentes de la infraestructura tecnológica debe estar registrado y se deben comunicar las políticas de buen uso y responsabilidad.

Incendios:

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

Es considerado el enemigo número uno de los equipos de cómputo ya que puede destruir fácilmente los archivos de información y programas.

Algunos factores a contemplar para reducir los riesgos de incendio:

- ✓ No debe estar permitido fumar en el área de proceso.
- ✓ Deben emplearse muebles incombustibles y cestos metálicos para papeles.
- ✓ El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.


Para protegerlos se debe tener en cuenta que en lo posible:

- ✓ La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- ✓ El centro de cómputo debe estar provisto de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- ✓ Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Recomendaciones

- ✓ El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
- ✓ Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes (cuarto de servidores).
- ✓ Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Inundaciones:

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Instalaciones Eléctricas:

Esta es una de las principales áreas a considerar en la seguridad física. En la medida que los sistemas se vuelven más complicados se hace más necesaria aplicar las soluciones que estén de acuerdo con una norma de seguridad industrial.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Es importante supervisar su disposición con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.


Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- ✓ **Interferencia:** estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- ✓ **Corte del cable:** la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- ✓ **Daños en el cable:** los daños normales con el uso pueden dañar el recubrimiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables
- ✓

Disturbios, Sabotajes internos y externos deliberados:

Para el control de acceso al cuarto de servidores a cualquier personal ajeno a la compañía se le tomarán los datos y se registrará el motivo de la visita, hora de ingreso y de salida.

El uso de carnét de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a las distintas áreas de la organización.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Otro mecanismo de seguridad, es el circuito cerrado de televisión; herramienta útil para el control y monitoreo de los espacios libres y algunos cerrados a fin de chequear el curso normal de actividades.

SEGURIDAD LOGICA:

Es importante recalcar que la mayoría de los daños que puede sufrir sistema de información no será sobre los medios físicos sino contra información por él almacenada y procesada. El activo más importante que se posee la compañía es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."


Los objetivos que se plantean son:

- ✓ Restringir el acceso a los programas y archivos de acuerdo al tipo de usuario
- ✓ Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizados los datos, archivos y programas correctos de acuerdo al correcto procedimiento.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido transmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. Por ejemplo: un buen canal de comunicación físico, por correo o telefónico.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información. Por ejemplo: servidores de respaldo.

CONTROLES DE ACCESO:

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de información y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION: 1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Los siguientes, son los requisitos mínimos de seguridad en cualquier sistema:

- ✓ Identificación y Autenticación
- ✓ Roles
- ✓ Transacciones
- ✓ Limitaciones a los Servicios
- ✓ Modalidad de Acceso
- ✓ Ubicación y Horario
- ✓ Control de Acceso Interno
- ✓ Control de Acceso Externo
- ✓ Administración

ANALISIS DE RIESGOS:

- ✓ El análisis supone obtener una evaluación del impacto de dichos sucesos negativos.
- ✓ El riesgo es la probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y periféricos.
- ✓ El valor calculado se utiliza para contrastar el costo de la protección de la información con el costo de una nueva producción

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

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


Grave: Es el 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.

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, routers, líneas telefónicas).
- ✓ Información
- ✓ Instalaciones

DEFINICION DE RIESGOS Y PLAN DE ACCION

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Riesgo	Descripción	Causa	Consecuencia	Acciones (Evitar el riesgo)
Fallas eléctricas. Electromagnetismo Sobrecarga eléctrica Falla de corriente (apagones)	El diseñado instalado y equipos encendidos producen una sobrecarga en cada línea y en las Ups existentes	Cableado eléctrico Sobrecargado de equipos. Condiciones no seguras del proveedor del servicio eléctrico. Condición física y ubicación geográfica del edificio	Daño en equipos. Pérdida de Información. Posibilidad de Incendio.	Monitorear y proponer si es el caso nuevos diseños de la red eléctrica y cambiar la actual con protectores tanto eléctricos como contra incendios. Adquirir e instalar una planta eléctrica. Instalar más estabilizadores y ampliar los puntos eléctricos.
Desactualización del Software de verificación estado de la red	Daños en equipos, software mal utilizado por los usuarios, cableado en mal estado, debido a mal funcionamiento de los programas que monitorean su funcionamiento	En la red de comunicaciones se pueden presentar problemas tecnológicos y humanos que hacen que la comunicación de información se haga muy lentamente por Mantenimientos mal hechos	Perdida de información Toma de decisiones errada, Desorden Pérdida de la confianza en el personal de tecnología Equipos desactualizados	Adquirir software confiable y seguro, con el fin de poder solucionar los problemas con la debida anticipación. Monitorear periódicamente los diagnósticos y estados de la red arrojados por el sistema, diligenciar bitácoras de control
Entrada física de personal no autorizado	Las personas ingresan a las instalaciones por visitas o reuniones establecidas	Implementación y mejora de de sistemas de seguridad y protocolos de acceso	Pérdida de elementos Perdida o daño de información Salida o conocimiento de	Mejorar los sistemas de seguridad que permitan verificar identidad y permisos de acceso de quien ingresa

PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA

CODIGO: TE-PR-02

VERSION:1.0

FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

			información confidencial	al área de sistemas y tecnología
Pérdida de información por virus informáticos Utilización de programas no autorizados / software 'pirateado'	Daño físico y lógico producido por condiciones físicas inapropiadas	Falta de mantenimientos preventivos Desconocimiento del personal técnico sobre estándares informáticos Descuido y falta de organización en los insumos e inventario de partes	Pérdida de información Daño en equipos	Planes de mantenimiento preventivo, periódicos. Capacitación al usuario sobre uso de equipos Monitoreo y supervisión de las condiciones físicas y lógicas Información actualizada resguardada en servidor, Actualización y mantenimiento del stock de partes y dispositivos
Manejo inadecuado de datos críticos (codificar, borrar, etc.) Transmisión no cifrada de datos críticos Manejo inadecuado de contraseñas (inseguras, no cambiar, BD centralizada)	Acciones erradas que causan pérdida de datos y falta de integridad Posibilidad de que se acceda, manipule y/o divulgue sin autorización	Falta de repaso de políticas Falta de control de tareas, funciones y responsabilidades definidas Inadecuado uso de metodologías de desarrollo y control sobre requerimientos del cliente Falta de definición de perfil, privilegios y restricciones Ausencia de	Falta de integridad de la información Pérdida de información Toma de decisiones errada Pérdida de la veracidad de los datos Mala imagen corporativa	Actualización de registros de desarrollo Uso de estándares de documentación de código fuente Actualización del diccionario de datos Aprobación y revisión de adquisición de software Protocolos de acceso y uso de base de datos y servidores

Uso indebido de la información		documentación Fraude interno Bajo nivel de seguridad para acceso		Administración de cuentas y roles de usuario Capacitación al usuario Encriptamiento Protocolo de interfaces de usuario y acceso
Vulnerabilidad de los sistemas de información	Posibilidad de que terceros entren de forma indebida o fraudulenta a los Sistemas de Información para alterar, hurtar o dañar la información	Cortafuegos inadecuados Falta de definición de perfil, privilegios y restricciones Bajo nivel de seguridad para el acceso a la información	Perdidas económicas Toma de decisiones errada Pérdida de la veracidad de los datos	Administración de cuentas y roles de usuario Encriptamiento Protocolo de interfaces de usuario y acceso a los Sistemas de información Monitoreo y control de accesos Actualización permanente de programas y paquetes de seguridad
Ausencia y/o deficiencia de las redes de voz y datos	Pérdida de la vigencia y disminución de la capacidad operativa de los equipos	Equipos activos y pasivos de red obsoletos	Perdidas económicas Pérdida de la comunicación interna y externa Inestabilidad de los procesos	Planes de mantenimiento preventivo periódicos Capacitación al usuario sobre uso de equipos Monitoreo y supervisión de las condiciones físicas de los equipos y redes Adecuado stock e inventario

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

FUNCIONES Y RESPONSABILIDADES

Responsable (persona o Cargo)	Funciones y responsabilidades
Asistente administrativo y tecnología	Responsable ejecución e implementación del plan Planear reuniones periódicas
	Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alternativo y comunicará a las directivas los costos para los gastos necesarios y el cronograma para la restauración del ambiente de trabajo.
	Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, Servicios de Internet, Intranet, correo electrónico y red
	Mantener actualizados dichos procedimientos en el Plan de Contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switches, antenas etc). Asimismo, deberá mantener actualizado el inventario de equipo de telecomunicaciones y redes,
Personal Operativo y administrativo	Es el responsable de llevar a cabo el inventario y mantenimiento de equipo escritorio, software y equipos periféricos, como impresoras, escáners, faxes, fotocopadoras, etc
	<p>Acotar el debido cumplimiento a las políticas de Tecnología, además de velar por el cuidado y buen uso de los equipos asignados por la compañía.</p> <p>Darán Aviso a la persona encargada de tecnología sobre cualquier anomalía, daño, incidente o accidente registrado en su equipo</p> <p>Cumplir con las acciones propuestas en el plan de contingencia informática</p>
Partes Interesadas, Asociadas de negocio	Durante su permanencia en las instalaciones deberá acogerse al debido cumplimiento de las políticas y normas de seguridad del área de tecnología de la compañía.

RECUPERACION Y RESTAURACION

Objetivos

- ✓ Permanente mantenimiento y supervisión de los sistemas y aplicaciones.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

- ✓ Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un evento.
- ✓ Puesta en marcha de las políticas y procedimientos para restaurar las aplicaciones y datos.
- ✓ Planificar la reactivación dentro de las 12 horas siguientes de producida una contingencia o un desastre, todo el sistema de procesamiento y sus funciones asociadas.

Alcance

Restablecer en el menor tiempo posible el nivel de operación normal del Sistema de información, basándose en los planes de emergencia y de respaldo y los demás que hayan establecido en la compañía.

Decisión

Queda a juicio del responsable y directivos determinar la activación del procedimiento y plan de contingencia informática, y además indicar el lugar alternativo de ejecución del Respaldo y/u operación de emergencia, basándose en las recomendaciones indicadas.

Duración estimada

Los dueños de proceso determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables) y en las fechas de realización de pagos y nómina.

Procedimientos de Respaldo y Recuperación

- ✓ Definir los procedimientos que indiquen los datos, programas, etc., que es importante respaldar; por servidor, sistema y ubicación.
- ✓ Identificar cada uno de los métodos que se utilizan, para llevar a cabo los respaldos de información, así como los procedimientos para su ejecución y restauración.
- ✓ Especificar el lugar donde se encuentran custodiados los respaldos de información o copia de los respaldos, ya sea en un lugar fuera de las instalaciones.

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION: 1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Se determinaron las prioridades de recuperación, en caso de falla o pérdida del Servidor con el que cuenta la compañía de la siguiente manera:

ALTA: Afecta directamente en las operaciones administrativas de la compañía y el proceso de operaciones y tráfico.
MEDIA: Afecta internamente a la compañía y no podría operar las áreas que utilizan los sistemas administrativos.
BAJA: No repercute en las operaciones de la Compañía

IDENTIFICACION DE EVENTOS Y MEDIDAS PREVENTIVAS

Las operaciones de SI LOGISTICA, pueden ser afectadas en menor o mayor medida por los distintos siniestros tanto naturales, accidentales o provocados.

Tomando en cuenta los resultados del Análisis de Riesgos realizado y los riesgos establecidos de acuerdo al SIG, se definieron los siguientes eventos para ser considerados en este Plan de Contingencia:

Movimiento Telúrico

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

CON PÉRDIDA DEL EDIFICIO: La pérdida de las instalaciones afectaría gravemente a las operaciones de la Sede y los datos pueden verse dañados seriamente.

En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

Incendio

ÁREA DE SISTEMAS: Se tiene gran impacto en la información ya que los sistemas utilizados residen dispositivos de almacenamiento, computadores, disco duros, equipos de comunicación y en caso de sufrir algún daño, se requerirá adquirir nuevos equipos, así como de instalar nuevamente los sistemas, configurar los sistemas y restaurar los respaldos para continuar trabajando.

ÁREAS DISTINTAS AL SITIO DE CÓMPUTO: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación, localizados en las áreas administrativas.

En el caso de las primeras el impacto que tendría es medio alto, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto, pero en el caso de las comunicaciones si pueden afectar en gran medida la operación del servicio

Inundación y Humedad

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

Un daño grave correspondería a una inundación en el área de Sistemas, en tanto que una inundación parcial o limitada a parte de las instalaciones, podría sólo ocasionar un daño medio si no va seguido de corto circuito.

Por otro lado, teniendo en cuenta la recuperación de los datos sería relativamente rápido aunque no sería lo mismo para el servidor o planta telefónica.

Corte de Energía

Las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño.

Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos.

Actualmente no se cuenta con una planta eléctrica, de manera que la capacidad de restablecer la energía inmediatamente después de la perdida de luz es nula. Los equipos cuentan con una UPS, para entrar inmediatamente después del corte de energía y evitar daños en los equipos.


Fallas en la red de Voz y Datos

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

Fallas en Hardware o Software

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

Sabotaje o Daño Accidental

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos.

Es posible que se requieran reprocesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles y del volumen de transacciones realizadas manualmente.

Vandalismo, Paro o Manifestaciones

Un intento de vandalismo ya sea menor o mayor, podría afectar a las PC's, periféricos y servidores así como las comunicaciones.

Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área de tecnología ya que puede dañar los dispositivos y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

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

1. Vigilancia mediante cámaras de seguridad, el cual registre todos los movimientos de entrada del personal.
2. Mantener la cultura de identificación de personal mediante el carné y estudiar la posibilidad de Instalar identificadores mediante tarjetas de acceso o huellas.
3. Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación. Mantener el servicio del sistema.
4. El paro total de las operaciones dentro de la Institución afectaría principalmente a los servicios que son proporcionados a los clientes, así como también las operaciones financieras.

Los principales conflictos que pudieran presentarse son:

- ✓ En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.
- ✓ Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro del área de tecnología, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc; por lo tanto es necesario mantener un sitio alterno

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

	PROCEDIMIENTO Y PLAN DE CONTINGENCIA INFORMATICA	
CODIGO: TE-PR-02	VERSION:1.0	FECHA DE ACTUALIZACION: 02 DE OCTUBRE DE 2017

Determinar lugares especiales, fuera de la sede, para almacenar los respaldos y copia de la documentación crítica.

El personal debe de dar la alerta del paro total y sacar la información y recursos que se hayan definido como vitales en un tiempo límite antes de ser declarada la huelga.

Junto con las directivas de la Institución se debe tener previamente definido un sitio alternativo para continuar con las operaciones críticas.

Asimismo, se tendrá que establecer un tiempo límite de espera de solución de la huelga como por ejemplo 24 horas con el fin de que no afecte el servicio proporcionado a los clientes y demás colaboradores de la compañía, si después de este intervalo la huelga continuara, se determinará el lugar o lugares de reubicación alternos

Control de cambios

Versión	Fecha	Aprobado	Descripción
1.0	02-10-2017	Gerencia General	Primera versión documento