Plan de contingencias.

Módulo de Supervisión de Contratos, Compras, Suministros y Servicios

Erik Francisco Arteaga

Jose Eduardo Maldonado

Gustavo Ramírez

Aura Cristina Valencia

SENA

Centro de biotecnología industrial

2013-2015

Índice.

[**INTRODUCCIÓN** 6](#_Toc414261416)

[**1.** **objetivos** 7](#_Toc414261417)

[**2.** **ventajas potenciales** 8](#_Toc414261418)

[**3.** **ALCANCE** 9](#_Toc414261419)

[**4.** **METODOLOGIA** 10](#_Toc414261420)

[4.1. Fase de Mitigación: 10](#_Toc414261421)

[4.2. Fase de Emergencia: 10](#_Toc414261422)

[4.3. Fase de Recuperación: 10](#_Toc414261423)

[4.4. Revisión: 10](#_Toc414261424)

[4.5. Evaluación del impacto por interrupción del servicio: 10](#_Toc414261425)

[4.6. Implementación: 11](#_Toc414261426)

[4.6.1. Cronograma: 11](#_Toc414261427)

[4.6.2. Documentación: 11](#_Toc414261428)

[4.7. Simulación o simulacro: 11](#_Toc414261429)

[4.8. Ejecución: 11](#_Toc414261430)

[**5.** **Identificación de analisís y riesgos** 12](#_Toc414261431)

[5.1. definicón: 12](#_Toc414261432)

[5.2. descripción y ánalisis de riesgos: 12](#_Toc414261433)

[5.2.1. riesgos con incidencia EXterna: 12](#_Toc414261434)

[5.2.2. Riesgos con incidencia interna: 12](#_Toc414261435)

[**6.** **IDENTIFICACION DE PROCESOS CRITICOS.** 15](#_Toc414261436)

[6.1. CRITERIOS PARA LA IDENTIFICACION DE PROCESOS CRITICOS: 15](#_Toc414261437)

[6.1.1. prioridad 1. 15](#_Toc414261438)

[6.1.2. prioridad 2. 15](#_Toc414261439)

[6.1.3. prioridad 3. 15](#_Toc414261440)

[6.2. factores criticos a considerar: 15](#_Toc414261441)

[6.2.1. aplicaciones en producción. 15](#_Toc414261442)

[6.2.2. personal: 16](#_Toc414261443)

[6.2.3. parque computacional y aplicaciones en uso: 16](#_Toc414261444)

[**6.3.** **NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECUROS INFORMATICO:** 16](#_Toc414261445)

[6.3.1. prioridad alta: 16](#_Toc414261446)

[6.3.2. prioridad media: 16](#_Toc414261447)

[6.3.3. prioridad baja 17](#_Toc414261448)

[6.3.4. Criticidad A: (Máxima) 17](#_Toc414261449)

[6.3.5. Criticidad B: (Intermedia) 17](#_Toc414261450)

[6.3.6. Criticidad C: (Mínima) 17](#_Toc414261451)

[6.4. PROCESOS CRÍTICOS 17](#_Toc414261452)

[6.4.1. ***SOFTWARE*** 17](#_Toc414261453)

[6.4.2. diagrama de red del centro de biotecnologia industrial sena. 19](#_Toc414261454)

[**7.** **PROCESO DE RESPALDO** 20](#_Toc414261455)

[7.1. Proceso de Respaldo Externo 20](#_Toc414261456)

[7.2. Plan de Backups y Equipos de Respaldo 20](#_Toc414261457)

Introducción.

Este documento contiene una serie de procesos, procedimientos y recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro, teniendo como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto en la organización y la menor pérdida de información posible.

El objetivo de este documento consiste en proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten.

El Plan está basado en un proceso dinámico y continúo que incluye no sólo las actividades a realizarse en el evento de una interrupción de la capacidad de procesamiento de datos; sino además, en las actividades realizadas anticipando dicho evento.

1. Objetivos

* Plantear y dotar a los funcionarios implicados en los distintos procesos del sistema de los procedimientos y elementos mínimos requeridos para afrontar la contingencia relacionada con el eventual cese de actividades, inoperatividad del sistema de información causada por razones de fuerza mayor.
* Proveer una solución para mantener operativo el sistema de información, que permita reducir el impacto en las operaciones normales cuando son interrumpidos o paralizados por contingencias que afectan parcial o totalmente los procesos normales que realiza o los datos que se procesan.
* Cuantificar la exposición a pérdidas asociadas a cada módulo del sistema de información, permitiendo un análisis de riesgos comprensible de los sistemas, que sirva como guía durante la ejecución del plan.
* Minimizar la posible pérdida operativa en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes. Así mismo, reducir las consecuencias de la posible pérdida de información relacionada con el evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.
* Mantener la prestación del servicio a los usuarios, en el nivel aceptable.
* Restablecer las operaciones del sistema en el menor tiempo posible, seguidos de cese, dependiendo de la anomalía que se presente.

1. Ventajas potenciales

El hecho de tener estructurado el plan de contingencias para el sistema de información S.A.M.I tiene algunas ventajas potenciales que ayudan a prevenir o a disminuir el impacto de los siniestros. Algunas de estas ventajas permiten:

• Determinar acciones preventivas que reduzcan el grado de vulnerabilidad; por el conocimiento que se tiene de los sistemas automatizados de información.

• Cuantificar los riesgos potenciales a que están expuestos al sistema de

Información.

• Facilitar la oportuna toma de decisiones ante anomalías o fallas.

• Contribuir a generar una cultura de seguridad y control en las áreas de sistemas e institucionalmente, haciendo énfasis en el manejo de la información.

• Asegurar la estabilidad operativa y de la organización, frente a la evidencia de un siniestro.

• Medir el grado de seguridad en el sistema de información.

1. Alcance

La necesidad de desarrollar un plan de contingencias, está relacionada con el impacto potencial que provoca la interrupción parcial o total del procesamiento de la información, sobre el normal desarrollo de las actividades del sistema de información S.A.M.I específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

Lo que supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, Software y Equipos electrónicos involucrados en los procesos críticos definidos en el Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del Centro de Cómputo principal de la entidad.

1. METODOLOGIA

Si las operaciones y procesos más importantes se encuentran automatizados en Gestión Documental, significa que el área de informática es de gran relevancia para el funcionamiento de la misma, lo cual obliga a la consideración de los siguientes aspectos:

El tiempo durante el cual la entidad puede funcionar sin sus recursos computacionales en operación.

La identificación de las amenazas potenciales sobre la capacidad de procesamiento automatizado de la información en la entidad.

La caracterización de las aplicaciones críticas que deben ser procesadas mientras se restablecen las operaciones normales en la entidad.

Tipificación de las consecuencias operativas, estratégicas, legales o de servicio, por la carencia del servicio automatizado.

El valor de la inversión en el desarrollo del plan de contingencias que asegure su continuidad y normal funcionamiento.

El Plan se ha estructurado en tres grandes Fases, a saber:

4.1. Fase de Mitigación: Gestión Documental, asegura la conservación de su información vital y determina donde procesar sus trabajos críticos de procesamiento de datos, sistemas o aplicaciones automáticas críticas, en caso de falla de sus equipos o de los mismos aplicativos.

4.2. Fase de Emergencia: Contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia.

4.3. Fase de Recuperación: Permite restablecer las condiciones originales y operación normal de los sistemas de información en su conjunto.

Los cuales implican el desarrollo de las siguientes Etapas:

4.4. Revisión: comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones de la misma.

4.5. Evaluación del impacto por interrupción del servicio: comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones. Esta evaluación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla el análisis de riesgos.

4.6. Implementación: se realizan actividades específicas para la reducción y eliminación de riesgos que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.

4.6.1. Cronograma: El diseño de un cronograma de trabajo provee la oportunidad de registrar los logros de cada tarea, verificar si las actividades han sido cumplidas o no en el tiempo previsto, y analizar cuáles han sido los principales inconvenientes que se han presentado si se detectan desviaciones importantes en el cronograma inicial, antes de la ejecución de las pruebas.

4.6.2. Documentación: Se prepararán y archivarán todos los documentos donde se registren las actividades, logros e inconvenientes, programas, objetivos, cronograma, procedimientos, planillas y todo aspecto fundamental referente a las acciones generadas durante el desarrollo del Plan de Contingencias, creando un historial de referencia.

4.7. Simulación o simulacro: se define el cronograma de simulacros, así como se designa a los responsables de dar inicio a las pruebas, ambientar el personal y los recursos, controlar los eventos, documentar las acciones y evaluar el resultado en su conjunto.

4.8. Ejecución: se sigue el desarrollo de:

* Medidas de protección planificadas por cada segmento afectado.
* Iniciación de las acciones destinadas, por prioridad, a controlar la situación durante los primeros instantes de la emergencia.
* Consideración de las responsabilidades extraordinarias que el comité directivo del plan tendría que asumir a fin de ofrecer protección y seguridad a los elementos materiales y humanos del área.
* Evaluación del estado del área de informática, poniendo en operación los procedimientos planificados para la recuperación total del servicio.

1. Identificación de análisis y riesgos

5.1 Definición.

Riesgo es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad, azar o exposición.

5.2 Descripción y análisis de riesgos:

El siguiente análisis de riesgos implica la valuación del impacto por interrupción del servicio, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones; esta evaluación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal de los sistemas de información con que cuenta la entidad, son entre otros:

Norma iso 27001

5.2.1. RIESGOS CON INCIDENCIA EXTERNA:

5.2.1.1. POLITICOS:

Modificaciones a la constitución política ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

5.2.2. Riesgos con incidencia interna:

5.2.2.1. Posible incumplimiento de los contratistas:

Este riesgo puede ocurrir a causa del posible atraso en la ejecución o trasgresión del clausulado de los contratos de actualización, modificación y mantenimiento, que se asumieron durante la validez del año en vigencia; para la aplicación de nómina, el Sistema Administrativo Modular Integrado SAMI.

5.2.2.2. Posibles retrasos en procesos administrativos:

La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos con exigencia en el cumplimiento de requisitos, ampliando el tiempo de ejecución de las actividades del Plan Emergente, de manera imprevista.

5.2.2.3 Contratación sin asistencia técnica, soluciones inadecuadas o incompatibilidad frente a los requerimientos y recursos disponibles:

Se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas, con el probable desconocimiento de las características, especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas, de manera compatible.

5.2.2.4. Posible pérdida de información:

Este riesgo tiene baja probabilidad de ocurrencia, si se tiene en cuenta que el Plan de contingencias incluye un proceso de respaldo, que permite la mitigación del riesgo, efectuando copias de seguridad (backups), tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros) como a los archivos de bases de datos y resultados de las aplicaciones específicas en producción para cada una de las dependencias de la Entidad.

5.2.2.5. Posible falla de equipos electrónicos y Hardware fuera de inventario:

Este riesgo se presenta por la Falta de Previsión, con la no inclusión de soluciones para aspectos de baja prioridad o al excluir elementos de los inventarios, por desconocimiento o por no haber sido reportados a tiempo a la Dirección de Informática.

5.2.2.6. Posibles fallas en el flujo de energía eléctrica:

Este riesgo está relacionado con amenazas externas al control de la Entidad. Sin embargo, se han implementado equipos para la mitigación del riesgo de corte temporal de energía eléctrica, dado que en el SENA está provista de UPS (Unidad de Poder In-interrumpido) en cada una de las redes de área local, para tener la posibilidad de salvaguardar la información durante aproximadamente una (1) hora. Si el corte es más prolongado, se debe acudir a los procedimientos de procesamiento en el centro alterno externo y en segunda instancia los procesos manuales establecidos como contingencia, hasta tanto no se solucione la falla.

La UPS actual funciona y cumple con su objetivo y tiene contrato de mantenimiento

5.2.2.7 Posible calentamiento de la sala de cómputo:

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que el SENA ha implementado procedimientos para su mitigación, tales como: La implementación en el centro de cómputo principal de un Sistema de Temperatura autorregulada, provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura, humedad, flujos de corriente, filtros de aire, alarmas local y silenciosa. Este sistema se encuentra conectado con la cámara principal a través de conductos que están en el piso para el control de los flujos de corriente y aire.

5.2.2.8 Posible falla de servicio telefónico:

Este riesgo está relacionado con amenazas externas al control de la Entidad, el SENA no puede efectuar mitigación de este riesgo. Sin embargo, se puede planear las posibles alternativas a implementar ante las posibles fallas del servicio telefónico. La probabilidad de ocurrencia sólo es manejable por la entidad proveedora del servicio.

El impacto sobre las operaciones del SENA es de nivel bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y redes locales implementada sobre cableado estructurado.

De otro lado, en lo que respecta al Centro de Cómputo principal del SENA, se desarrolló un análisis del medio y los procedimientos de seguridad y control existentes.

1. Identificación de procesos críticos.
   1. Criterios para la identificación de procesos críticos:

El informe administrativo o plan de contingencia se considera “requerido” para todos los sistemas de prioridad 1 “recomendables” para todos los sistemas de prioridad 2 y “sugeridos” para todos los sistemas de prioridad 3.

* + 1. Prioridad 1.
* Todos los sistemas vitales de la organización.
  + 1. Prioridad 2.
* Sistemas con múltiples interfaces.
* Procedimientos o dispositivos que no pueden ser sometidos a pruebas.
* Medios que alimentan datos a los sistemas vitales.
  + 1. Prioridad 3.
* Sistemas cuya falla causa molestia a menores.
  1. Factores críticos a considerar:
     1. Aplicaciones en producción.
* nivel de importancia de la aplicación en la entidad.
* Impacto operativo, financiero o contable.
* Oportunidad de procesamiento.
* Programas críticos.
* Comunicaciones: entrada y salida de datos.
* Implicaciones para el usuario en caso de ausencia del recurso aplicativo.
* Documentación del sistema: manuales de usuario y procedimientos de operación.
* Procedimientos de respaldo y recuperación a nivel aplicativo.
  + 1. Personal:
* Funcionarios de posición clave y personal de dirección.
* Personal con alta dependencia en los sistemas automatizados.
* Personal de respaldo.
* Entrenamiento.
  + 1. Parque computacional y aplicaciones en uso:
* Servidores, computadores personales, impresoras, periféricos, etc.}
* Líneas de comunicación y equipos relacionados.
* Sistemas operativos y programas producto.
* Suministros: papel, formas continuas.
  1. Niveles de prioridad y criticidad de los recursos informáticos:

Teniendo en cuenta los criterios de factores enunciados anteriormente, se han definido los siguientes niveles de prioridad y criticidad de los recursos informáticos con los que cuenta el SENA.

* + 1. Prioridad alta:

Corresponde a todas aquellas herramientas del SENA, que en el caso de no ser adaptadas oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar la actividad del centro.

* + 1. Prioridad media:

Se le asigna a las diferentes áreas del SENA, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de control, cuentan con procedimientos alternativos preestablecidos.

* + 1. Prioridad baja

Se le asigna a todas aquellas herramientas (impresoras, computadores, IP) del SENA, cuya falta de adaptación no representa graves traumatismos y sus modificaciones pueden aplazarse para la última parte del proyecto.

* + 1. Criticidad a: (máxima)

El aplicativo no puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas

* + 1. Criticidad b: (intermedia)

No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles. Ante esta situación debe remplazarse parcialmente por un proceso manual.

* + 1. Criticidad C: (Mínima)

Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles. Debe sustituirse temporalmente por un proceso manual.

* 1. Procesos críticos

Con base en lo anterior, se establecieron los procesos críticos del SENA descritos en la siguiente relación de recursos informáticos señalando la prioridad y las acciones a seguir para cada problemática en particular.

* + 1. Software
       1. Software aplicativo
          1. Aplicaciones de desarrollo externo

Se determinó que las aplicaciones en producción que presentan un alto riesgo de pérdida de información y que pueden provocar parálisis en los procedimientos administrativos (en caso de no ser debidamente adecuadas), son aquellas elaboradas e implementadas a través de procesos contractuales; por lo tanto, serán objeto de inmediata solución.

* + - * 1. Aplicaciones de Desarrollo Interno

La dirección de informática ha desarrollado aplicaciones que actualmente operan en la entidad, para las cuales se han iniciado procesos de adecuación y prueba bajo la responsabilidad de instructores asignados.

* + 1. Diagrama de red del centro de biotecnología industrial SENA.

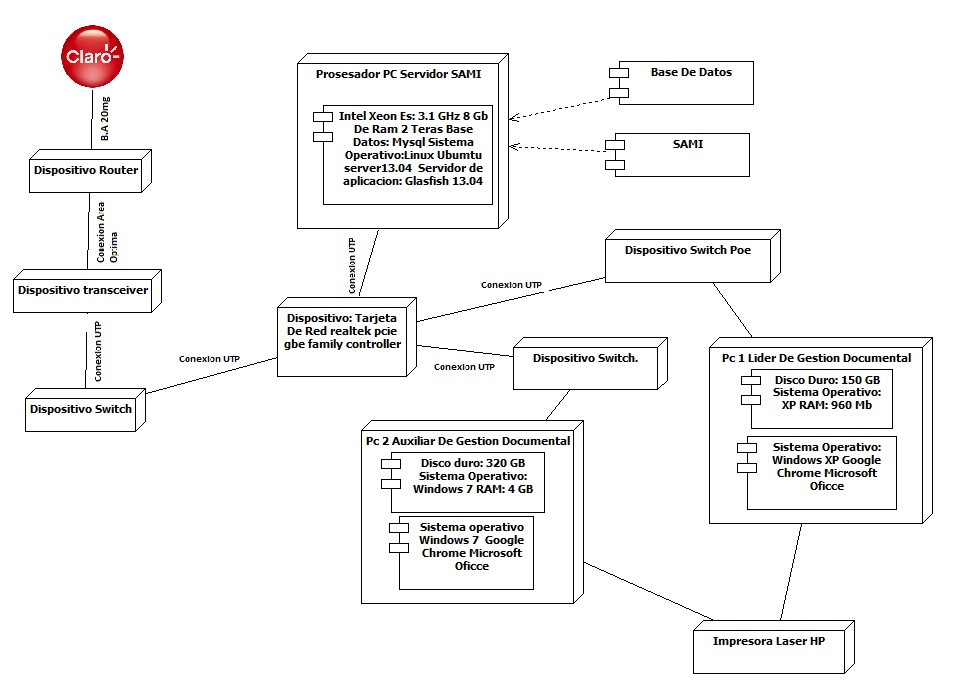
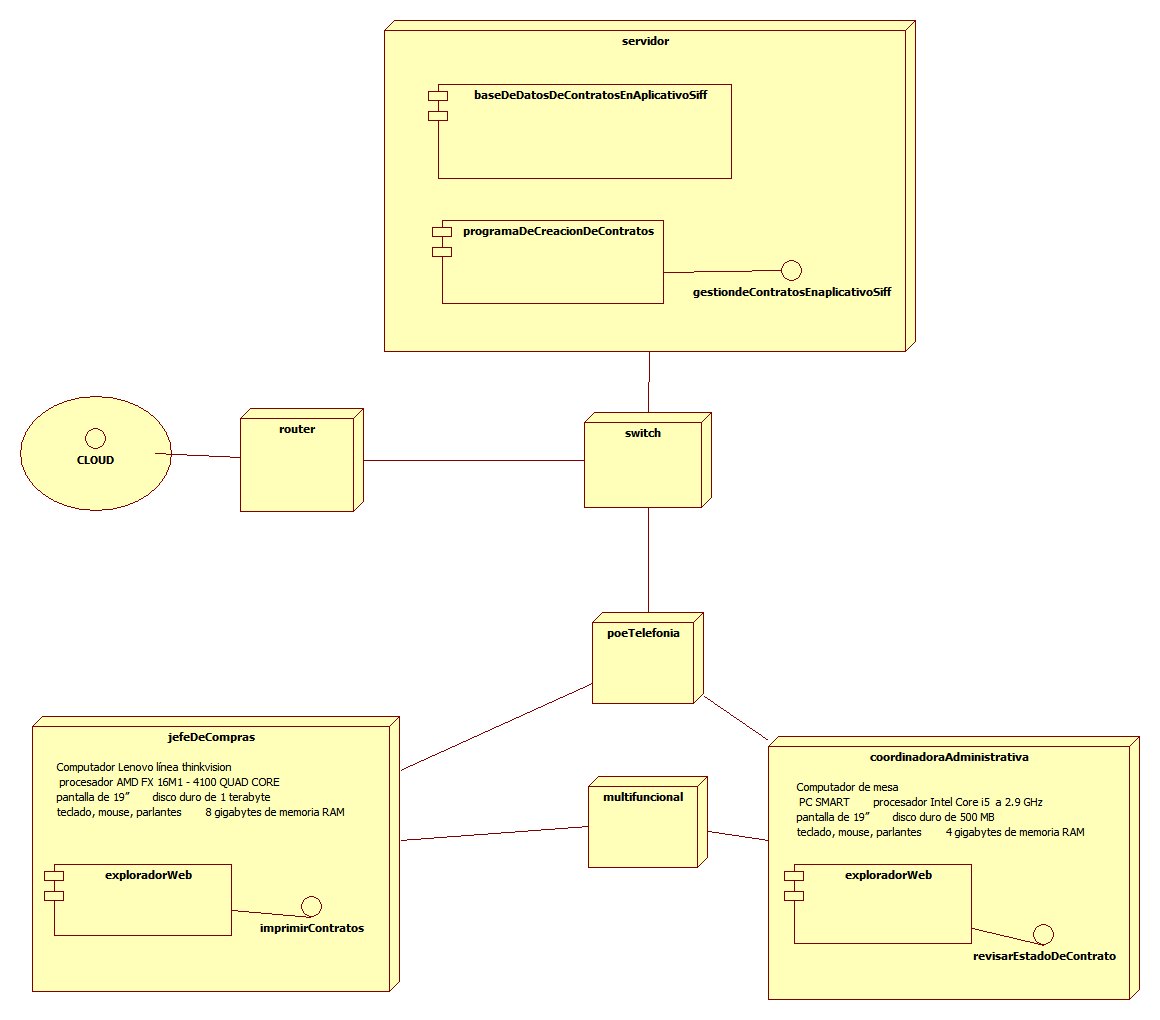


Ilustración . diagrama de red

1. Proceso de respaldo

El Proceso de Respaldo establecido como procedimiento de Mitigación, a través del cual el SENA asegura la conservación de su información vital y determina donde realizar sus trabajos críticos de procesamiento de datos en caso de falta o falla de sus equipos.

El diseño del proceso de respaldo incluye los cinco (5) principales componentes de un sistema de información, a saber:

* Los datos
* La documentación
* Los programas (software)
* Los procedimientos
* Los equipos (hardware)
  1. Proceso de Respaldo Externo

Como sitio de respaldo externo se entiende una instalación diferente a la sede principal de la entidad donde se almacena una copia de los archivos de backups de la entidad, para que ante cualquier eventualidad que se presente en la sede principal se pueda reiniciar labores con los archivos almacenados en el sitio de respaldo externo.

* 1. Plan de Backups y Equipos de Respaldo

Un backup es una copia de seguridad de la información en un segundo medio que nos garantiza recuperar la información contenida en nuestras maquinas en caso de que se presente alguna falla en el disco duro, un borrado accidental o un accidente imprevisto.

Estos backup deben ser ejecutados por:

1. El administrador del centro de computo
2. Usuarios con privilegios para realizar copias de seguridad.