Plan de Continuidad del Negocio

Metodología recomendada para pequeñas empresas

16/03/2010

INFORMACIÓN SOBRE REVISIÓN DEL ENTREGABLE

Versión	Elaborado Por	Fecha Generación	Firma	Comentarios adicionales
1.0	Rodrigo Ferrer CISSP, CISA, CSST, ABCP, ISO 27001 L.A AMBCI, COBIT 5.0	09-2-2010		N/A

INFORMACIÓN SOBRE APROBACIÓN DEL ENTREGABLE

Versión	Revisado Por	Fecha de Revisión	Firma de Aprobación	Comentarios adicionales
1.0		09-2-2010		N/A

INFORMACIÓN SOBRE CONTROL DE VERSIONES

Versión	Fecha de Actualización	Elaborado Por	Revisado por	Comentario adicionales
1.0	13-2-2010			Versión inicial

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. INTRODUCCIÓN

En los últimos años, las entidades a nivel nacional han concedido una importancia creciente a la implementación de planes, procedimientos, y estructuras que garanticen la continuidad de sus procesos críticos de negocio ante eventualidades de diversas categorías y diferentes niveles de impacto. Estos factores, junto con una legislación cada vez más exigente en lo relacionado a la confiabilidad en la prestación de servicios, han llevado a que en la actualidad la presencia de estos planes sea un factor común.

Planes de Contingencia

En la Figura No. 1, basada en la publicación especial del NIST, SP800-34, se observa cómo diferentes planes de contingencia (PCN) se relacionan con el Plan de Continuidad del Negocio o BCP por sus siglas del inglés:

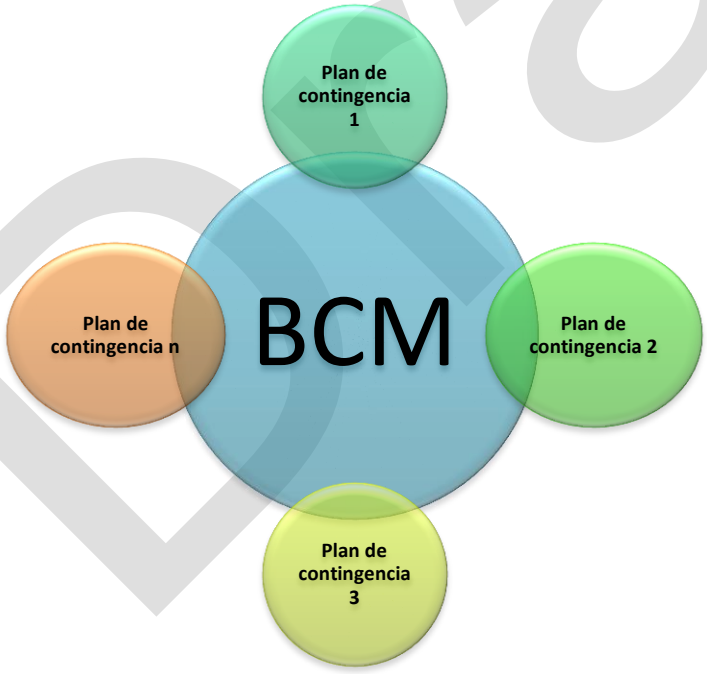

Figura No. 1. Planes de contingencia y BCP.

Según el NIST, los Planes de Contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI después de una emergencia. Es posible en algunos casos contar con múltiples Planes de Contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia serán parte del BCP.

2. OBJETIVO DE LOS PLANES DE CONTINGENCIA

El objetivo del Plan o Planes de Contingencia es sostener en niveles previamente definidos y aceptados, las operaciones y servicios de Tecnologías de Información (TI) a través de la estructuración de procedimientos e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre. También para el caso de componentes, sistemas o servicios críticos se puede contar con uno o más planes de contingencia los cuales se anexarán al BCP.

3. ALCANCE DEL PROYECTO

El alcance de los planes de contingencia se determina con base en los sistemas o activos críticos de TI. Estos se definen con base en los procesos críticos del negocio que son definidos durante el Análisis de Impacto al Negocio (BIA) desarrollado durante el BIA del BCP.

4. METODOLOGÍA

La metodología utilizada para el desarrollo de los Planes de Contingencia, propone un proceso comprendido desde la definición de la política de contingencia hasta el mantenimiento del plan. Esta metodología, está apoyada en mejores prácticas a nivel internacional proveniente de reconocidos institutos tales como el NIST SP800-34, El DRII, ISO 27001, NFPA 1600, entre otros. La Figura No. 2 presenta las fases de esta metodología:

1. Definir la política de contingencia
2. Análisis de impacto al negocio (BIA, Business Impact Analysis, por sus siglas del inglés)
3. Identificación de controles preventivos
4. Desarrollo de estrategias de recuperación
5. Desarrollo del plan de contingencia
6. Entrenamiento
7. Pruebas
8. Auditoría

9. Mantenimiento del plan

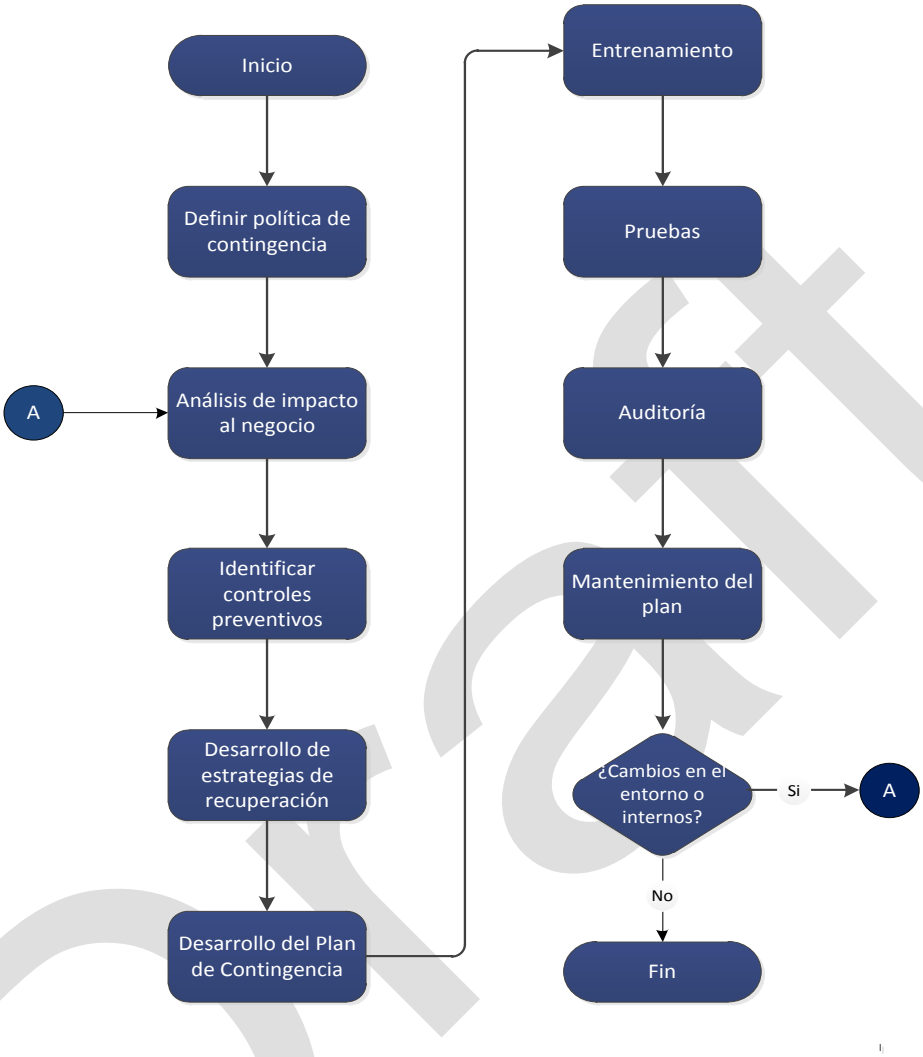

Figura No. 2 Fases de la metodología del PCN.

Este documento desarrolla los siguientes aspectos para cada una de las fases de la metodología propuesta:

- Una descripción de cada una de las fases, su propósito y alcance.
- Información de las entradas, actividades que se realizan, su secuencia, y los productos o salidas que se generan.

5. DEFINIR LA POLÍTICA DE CONTINGENCIA

Con el fin de garantizar la efectividad y el entendimiento por parte del personal de los requerimientos de continuidad de las operaciones de TI, el plan debe estar basado y apoyado en una política claramente definida y posteriormente aprobada formalmente. Entre los elementos principales a los que debe estar orientado esta política se tienen:

1. Roles y responsabilidades
2. Objetivos
3. Requerimientos en general
4. Alcances
5. Recursos requeridos
6. Requerimientos de entrenamiento
7. Periodicidad de las pruebas del plan
8. Periodicidad del mantenimiento

6. ANÁLISIS DE IMPACTO AL NEGOCIO

El propósito del Análisis de Impacto al Negocio, conocido comúnmente como BIA, es caracterizar los diferentes sistemas, procesos e interdependencias y con base en esto definir los requerimientos y prioridades para el PCN. El propósito del BIA es correlacionar los componentes de un sistema con los servicios críticos que ellos soportan y así poder determinar las consecuencias de una interrupción o emergencia. Por otra parte, el BIA permite estimar los tiempos objetivos de recuperación de los procesos críticos con el fin de regresarlos a su operación normal después que ha ocurrido un desastre y los tiempos de almacenamiento requeridos para disminuir la pérdida de datos.

El BIA implica determinar las labores y los recursos esenciales para respaldar la continuidad de las operaciones de TI, su criticidad, su impacto para el negocio, sus RTO´s (Recovery Time Objective - tiempo de recuperación objetivo)[1] y RPO´s (Recovery Point Objective - punto de recuperación objetivo)[2].

[1] RTO: lapso de tiempo en el cual debe restaurarse el proceso después de un desastre.

[2] RPO: punto en el tiempo a partir del cual los datos deben ser restaurados. Transacciones después de este tiempo deben ser capturadas a mano o a partir de los esquemas de contingencia. Esta es una definición general de lo que se denomina "pérdida aceptable" en una situación desastrosa.

Para el desarrollo de esta fase se emplean encuestas, diligenciadas por expertos de los sistemas o componentes de TI de SISTESEG, y se desarrollan entrevistas para aquellos casos en que las respuestas a las encuestas requieran precisarse o cuando los encuestados soliciten ayuda para su diligenciamiento.

En la Figura No. 3, se presentan las actividades, entradas y productos relacionados con la metodología del BIA:

1. Planeación del BIA
2. Levantamiento de la información
3. Identificar activos o sistemas críticos de TI
4. Identificar Impactos, RTO y RPO
5. Desarrollar prioridades de recuperación
6. Análisis de la información
7. Informe de resultados

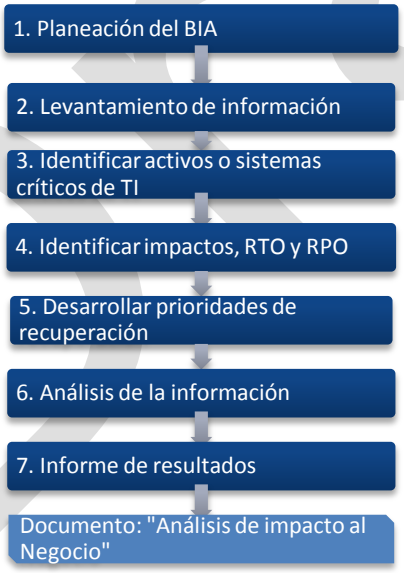

Figura No. 3 Actividades del BIA.

6.1 Planeación del BIA

En esta fase se planea la estructura conceptual para el desarrollo de las fases posteriores y se diseñan también los formatos de los documentos requeridos en cada una de estas fases:

1. Entender previamente los procesos del negocio de SISTESEG sobre los que se realizará el BIA.
2. Entender los sistemas o componentes de TI
3. Definir qué aspectos del negocio se desean cubrir con la información que se suministrará.
4. Identificar el personal a ser entrevistado.
5. Definir los cuestionarios a utilizar para recolectar la información, capacitar a los entrevistadores, unificar criterios y términos utilizados.
6. Definir las fechas en que se realizarán las entrevistas.

6.2 Levantamiento de información

En esta fase se realizan las entrevistas con el objetivo de recolectar la información necesaria para ser utilizada en las actividades posteriores.

1. Realizar las entrevistas utilizando los cuestionarios diseñados en la fase de Planeación.
2. Inspeccionar físicamente los sitios.
3. Solicitar diagramas de red y servidores
4. Verificar a través de preguntas adicionales otros componentes de TI.

6.3 Identificar activos o sistemas críticos de TI

Los sistemas de tecnologías de información puede ser muy complejos debido a la gran cantidad de interdependencias que pueden tener en elementos de software y de hardware. En esta actividad se trata de analizar los diferentes sistemas de TI con el fin de determinar las funciones o servicios críticos que se desprenden de ellos y también se busca identificar elementos críticos requeridos para realizar estas funciones o prestar estos servicios (ver Figura No. 4).

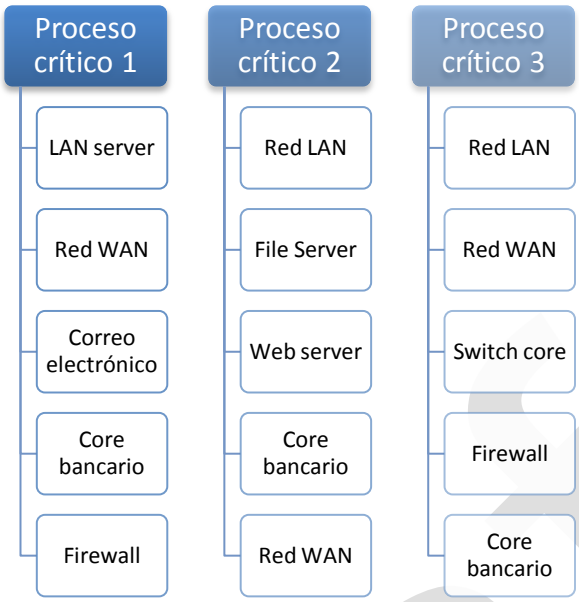

Figura No. 4 Identificación de activos críticos.

Se puede complementar esta actividad (identificación de activos) con la realización de diagramas de dependencia que nos indican la conformación y criticidad de ciertos elementos de un sistema, tal como se muestra en la Figura No.5.

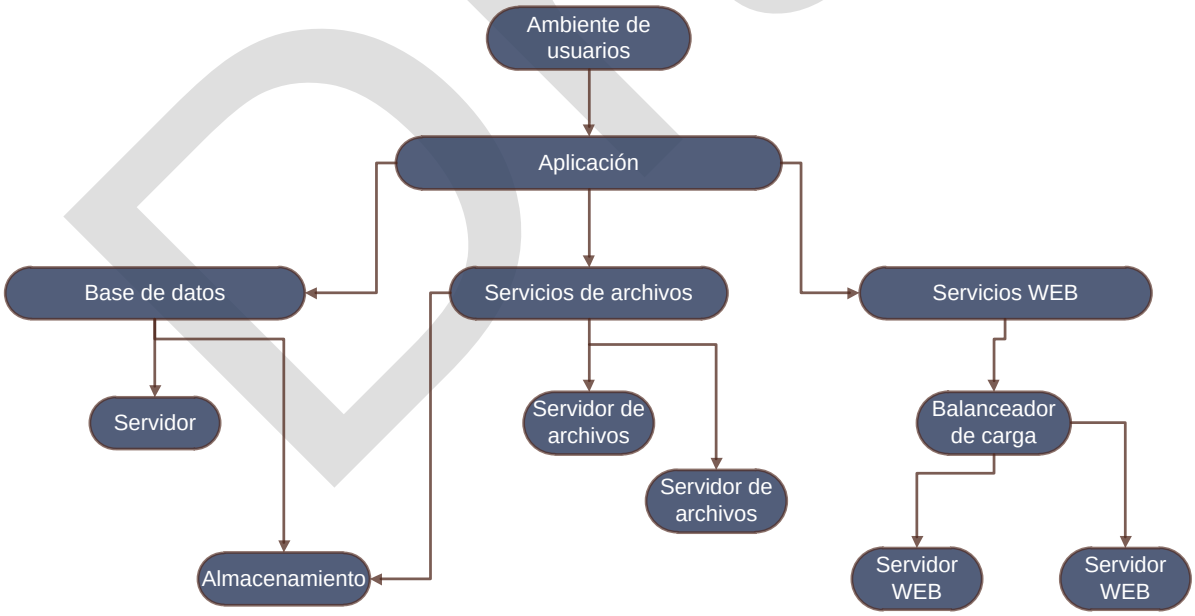

Figura No. 5 Diagrama de dependencia.

También se puede complementar esta actividad con la realización de diagramas (árboles) de fallas que nos indican la conformación y criticidad de ciertos elementos de un sistema y cuál sería el impacto de que alguno de estos elementos fallen, tal como se muestra en la Figura No.6.

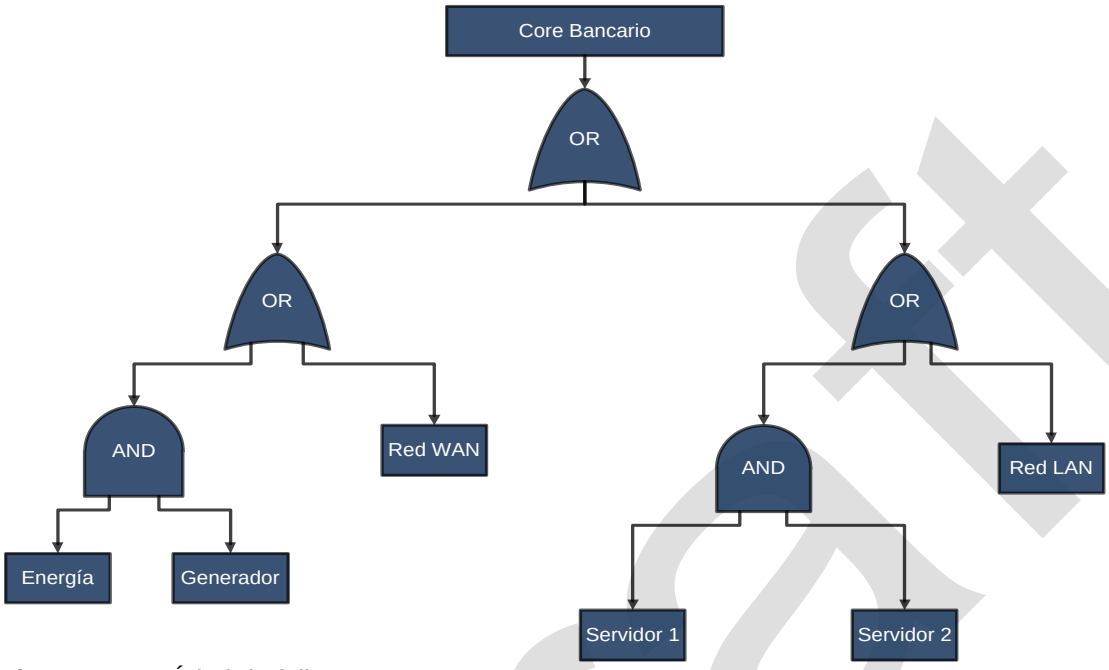

Figura No. 6. Árbol de falla.

6.4 Identificar impactos, RTO y RPO

En esta actividad se deben determinar los impactos en las operaciones de TI si un determinado activo fuera dañado o interrumpido. Este estudio debe evaluar los impactos de dos maneras:

1. El efecto de la falla debe ser estudiado en el tiempo con el fin de identificar los RTO´s y los RPO´s.
2. Los efectos de la falla deben ser estudiados considerando los recursos y dependencias, con el fin de identificar efectos cascada a lo largo del sistema considerado como parte del plan de contingencia.

Figura No. 7 Determinación de RTO´s.

6.5 Desarrollar prioridades de recuperación

Los tiempos de recuperación objetivos y los impactos definidos en la anterior actividad serán la base para definir y priorizar las estrategias de recuperación que serán consideradas cuando de implementar el plan se trate en una fase posterior. Si para el caso del servidor de archivos se determinó que el tiempo de recuperación deber ser de 8 horas, medidas conducentes a lograr este tiempo deben ser tomadas ya sea en la adquisición de hardware o software, alquiler o acuerdos de servicios con proveedores, entre otras.

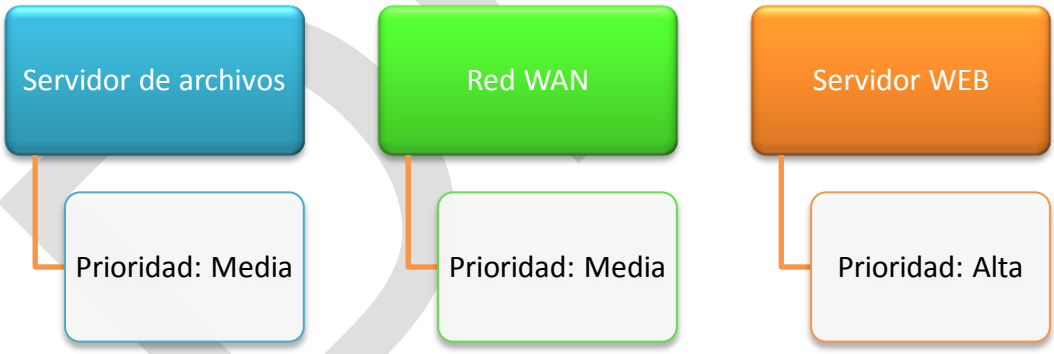

Figura No. 8 Prioridades de recuperación.

6.6 Informe de Resultados

Una vez recolectada y analizada la información se genera un reporte con los principales hallazgos (observaciones). Mediante el informe del BIA se pretende mostrar el resultado que arroja el análisis de la información.

1. Presentar la clasificación de los activos o sistemas críticos

2. Presentar consolidados de RTO´s
3. Presentar consolidados de RPO´s
4. Presentar activos o sistemas críticos
5. Presentar los activos que tendrán que ser adquiridos (reposición) como consecuencia de un posible desastre.
6. Presentar las prioridades de recuperación
7. Generar observaciones sobre los resultados obtenidos.

6.7 Estructura del documento

La estructura o contenido del documento *Análisis de Impacto* se expone a continuación:

1. Objetivo
2. Alcance
3. Sistemas o activos de TI seleccionados
4. Metodología
5. Personal entrevistado
6. Análisis de la información
7. Informe de resultados

Figura No. 9. Estructura del documento.

7. IDENTIFICAR CONTROLES PREVENTIVOS

El propósito principal de esta fase es conocer cuáles amenazas o riesgos específicos enfrenta SISTESEG en sus procesos críticos del negocio, identificados como resultado del Análisis de Impacto al Negocio (BIA), con el fin de determinar la forma en que algunos riesgos serán controlados y mitigados a un nivel aceptable según criterios previamente definidos.

Es conveniente mencionar que durante esta fase los riesgos (operativos) se analizarán desde la perspectiva de la continuidad del negocio considerando activos de TI, sin dejar de lado su relación directa con los procesos determinados como críticos. El tipo de vulnerabilidades y amenazas al que se ven expuestos estos activos varía dependiendo de la naturaleza de los mismos. Las amenazas y vulnerabilidades que se incluyen para el caso específico del proyecto, serán las relacionadas con la no disponibilidad (operación) de los activos asociados a los procesos críticos del negocio.

En la Figura No. 10 se observan las actividades que se desarrollan en esta fase, las cuales serán explicadas en lo que sigue de este documento.

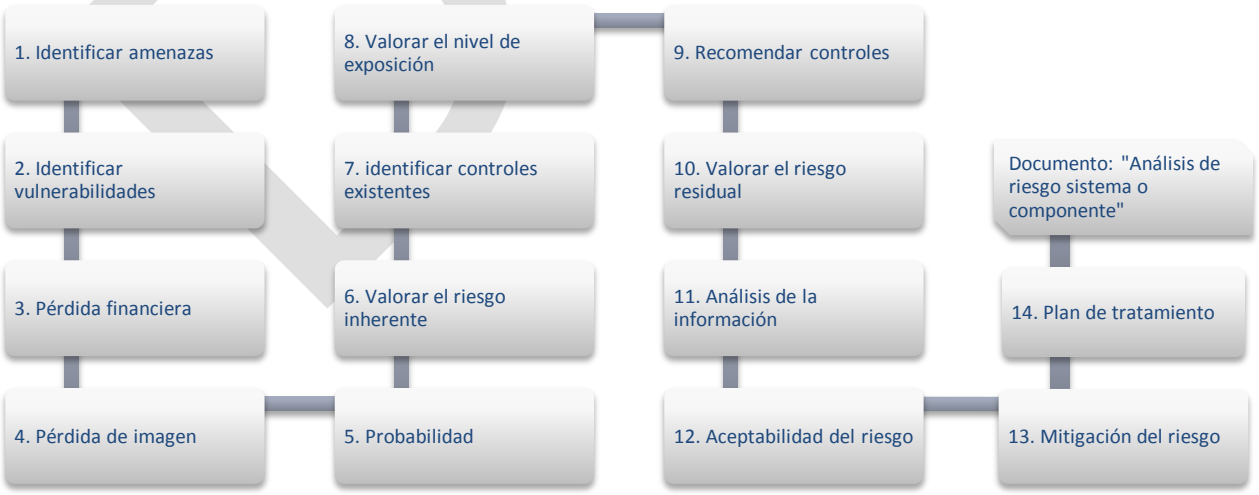

Figura No. 10. Actividades de la fase de evaluación de riesgos.

7.1 Identificar amenazas

Las amenazas pueden ser el resultado de actos deliberados o mal intencionados que afectan los activos de los procesos. Las organizaciones enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los activos de TI se realizarán entrevistas con expertos de SISTESEG, quienes suministrarán información sobre cuáles son las amenazas con mayor impacto desde la perspectiva de continuidad del servicio o servicios de TI, las que podrían llegar a afectar la continuidad de las operaciones de TI, y por consiguiente, podrían causar una pérdida financiera o afectación de la imagen de la compañía.

Una vez identificadas las amenazas, y con el propósito de complementar y de validar la lista de amenazas encontradas, se realiza una verificación contra algunas de las fuentes de amenazas especificadas en Figura No. 11. **Fuentes de amenazas.**, agrupándolas para el análisis de riesgo como amenazas de tipo natural, intencionales (humanas) o accidentales.

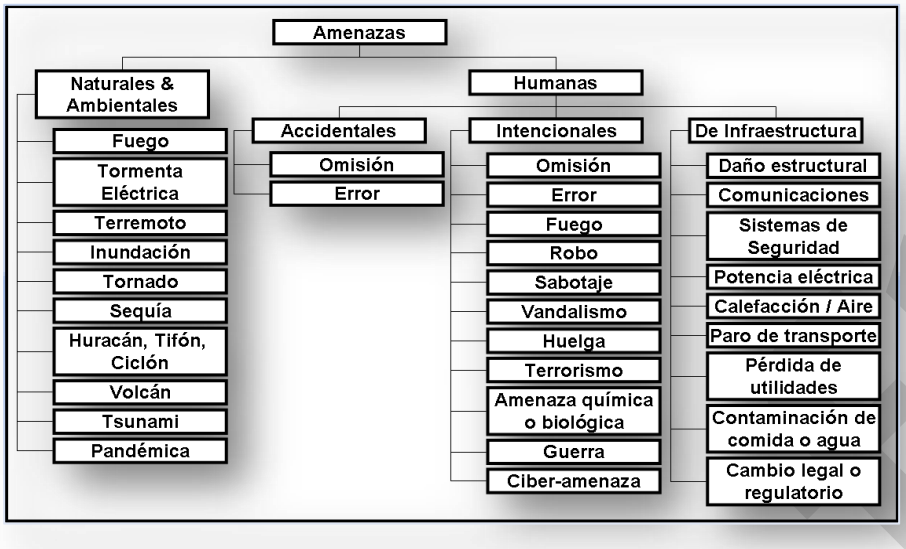

Figura No. 11. Fuentes de amenazas.

7.2 Identificar vulnerabilidades.

En esta actividad se establece el conjunto de vulnerabilidades que posee cada activo crítico de TI, que en caso de ser explotadas por una o varias amenazas, afectarían la continuidad de las operaciones. Las vulnerabilidades, por su parte, son debilidades o ausencia de controles que un activo perteneciente a un proceso pueda tener.

Algunas vulnerabilidades consideradas dentro de esta metodología son:

1. Ausencia de políticas
2. Configuraciones no seguras
3. Errores de configuración.
4. Errores de mantenimiento.
5. Errores del administrador.
6. Errores en código.
7. Exposición a materiales peligrosos.
8. Fallas de usuarios.

9. Manuales de uso no documentados
10. Medidas de protección de acceso inadecuadas
11. Medidas de protección física inadecuadas
12. Procesos o procedimientos no documentados.
13. Usuario desinformado.
14. Tecnología inadecuada.
15. Debilidad o inexistencia de controles.
16. Condiciones de locales inadecuadas o no seguras.

7.3 Valorar la pérdida financiera (PF)

Se debe seleccionar un valor de 1 a 3, considerando las descripciones que se especifican en la Tabla No. 1. Escalas definidas para la Pérdida Financiera (PF)., para así poder evaluar los diferentes riesgos más adelante.

Valor	Descripción
3	Más de $100'000.001
2	$30.000.001-$100'000.000
1	$0 - $30.000.000

Tabla No. 1. Escalas definidas para la Pérdida Financiera (PF).

7.4 Valorar la pérdida de imagen (PI)

Se debe seleccionar un valor de 1 a 3, considerando las descripciones que se especifican en la Tabla No. 2. **Escalas definidas para la Pérdida en la Imagen**

Valor	Descripción
3	Pérdida de imagen a nivel nacional
2	Pérdida de imagen a nivel departamental
1	Pérdida de imagen a nivel clientes SISTESEG

Tabla No. 2. Escalas definidas para la Pérdida en la Imagen (PI).

7.5 Valorar la probabilidad (PR)

La probabilidad de que una vulnerabilidad potencial pueda ser explotada o aprovechada por una amenaza es clasificada como alta, media o baja. A continuación se describen estos tres niveles de probabilidad de la amenaza. Se debe seleccionar un valor de 1 a 3, considerando las descripciones que se especifican en la Tabla No. 3. Escalas definidas para la Probabilidad (PR).

PR	Descripción
3	**Alta.** Casi cierta**,** la expectativa de ocurrencia se da en todas las circunstancias. La amenaza se presenta con alta frecuencia.
2	**Media.** Moderada**,** puede ocurrir. La amenaza se presenta con frecuencia media.
1	**Baja.** Rara**,** puede ocurrir sólo bajo circunstancias excepcionales. La amenaza no se presenta o se presenta con baja frecuencia.

Tabla No. 3. Escalas definidas para la Probabilidad (PR).

7.6 Valorar el riesgo inherente (RI)

Para valorar el riesgo inherente, se asignan las siguientes calificaciones: pérdida financiera (PF), pérdida de imagen (PI) y probabilidad (PR), según las tablas 1,2 y 3. Al asignar las calificaciones al riesgo inherente se debe considerar que el activo no cuenta con controles para mitigar el impacto o reducir la probabilidad.

El valor del riesgo inherente se obtiene al aplicar la siguiente fórmula:

(1) RI = (PF + PI) * PR

En la Tabla No. 4. Escalas definidas para el Riesgose observa la relación de criticidad del riesgo contra los valores alcanzados.

Valores alcanzados	Descripción
18-12	Alto
11-7	Medio
6-2	Bajo

Tabla No. 4. Escalas definidas para el Riesgo Inherente (RI).

7.7 Identificar controles existentes

El objetivo de esta actividad es determinar si las vulnerabilidades de disponibilidad de los activos asociados a los procesos están siendo mitigadas por los controles implementados actualmente. Se considera la lista de controles preventivos, detectivos, correctivos y disuasivos implementados para el activo. A continuación se presentan ejemplos de posibles controles existentes:

1. Se cuenta con fuente de poder redundante
2. Se cuenta con algunas medidas de seguridad física
3. Se tiene personal de administración
4. Se realiza monitoreo desde España
5. Se cuentan con repuestos de hardware el siguiente día hábil
6. Se cuenta con ingeniero de soporte local
7. Se hace respaldo a disco duro externo
8. Se monitorea los recursos de los servidores localmente
9. Se realiza inventario automatizado de hardware y software
10. Se tienen plantillas de configuración segura
11. Se realiza análisis de disponibilidad y capacidad local

7.8 Valorar el Nivel de Exposición (NE)

La existencia de controles relacionados a una vulnerabilidad permite reducir el nivel de riesgo asociado a la misma (a mayores controles implementados, menor es el nivel de exposición a

esa vulnerabilidad). Se califica el impacto y la probabilidad de exposición (considerando los controles existentes) de cada uno de los riesgos identificadas, empleando las tablas de calificación de impacto y de probabilidad previamente definidas.

El valor del nivel de exposición se obtiene al aplicar la siguiente fórmula:

(2) NE = (PF + PI) * PR

En la Tabla No. 5. Escalas definidas para el Tabla No. 4. Escalas definidas para el Riesgose observa la relación de criticidad del riesgo contra los valores alcanzados.

Valores Alcanzados	Descripción
18-12	Alto
11-7	Medio
6-2	Bajo

Tabla No. 5. Escalas definidas para el Nivel de Exposición (NE).

7.9 Recomendar controles

Se proponen controles para las vulnerabilidades que se encontraron durante el desarrollo de las entrevistas. Para esto nos apoyamos en mejores prácticas internacionales tales como ISO 27001, ISO 27005, ITIL v3, COBIT 4.1, EIA-TIA 942, NFPA 75, entre otras. Ejemplos de controles recomendados son:

1. Implementar un sistema de gestión de la seguridad
2. Contar con una gestión de la capacidad formal de los servidores
3. Contar con una gestión de la disponibilidad formal de los servidores
4. Contar con un DRP
5. Contar con un sistema de clasificación de la información
6. Contar con un sistema de gestión ISO 27001:
    a. A.5 Política de seguridad
    b. A.6 Organización de la seguridad de la información
    c. A.7 Gestión de activos
    d. A.8 Seguridad en el recurso humano
    e. A.9 Seguridad física y ambiental
    f. A.10 Gestión de las comunicaciones y operaciones
    g. A.11 Control de acceso

h. A.12 Adquisición, desarrollo y mantenimiento de sistemas de información
i. A.13 Gestión de incidentes de seguridad
j. A.14 Gestión de la continuidad del negocio (bcp/bcm)
k. A.15 Cumplimiento

7. Contar con estándares de seguridad física en el centro de cómputo
8. Contar con inventario de servidores actualizado
9. Contar con diagramas de red actualizados
10. Contar con un sistema de monitoreo formal sobre la red

7.10 Valorar el Riesgo Residual (RR)

Se califica el impacto y la probabilidad residual (considerando los controles recomendados) de cada una de las amenazas y riesgos identificados, empleando las tablas de calificación de impacto y de probabilidad previamente definidas con el propósito de determinar la efectividad de los controles recomendados.

El valor del riesgo residual se obtiene al aplicar la siguiente fórmula:

(3) RR = (PF + PI) * PR

En la Tabla No. 6. Escalas definidas para el riesgose observa la relación de criticidad del riesgo contra los valores alcanzados.

Valores alcanzados	Descripción
18-12	Alto
11-7	Medio
6-2	Bajo

Tabla No. 6. Escalas definidas para el riesgo residual (RR).

7.11 Análisis de la información

Para el análisis de la información se tendrá en cuenta por un lado la probabilidad asociada al riesgo, y por el otro, el impacto asociado a este riesgo. Las zonas que aparecen en color rojo y amarillo serán las zonas de riesgo inaceptable.

		Impacto		
		Bajo	Medio	Alto
Probabilidad	Alta	Medio	Alto	Alto
	Media	Bajo	Medio	Alto
	Baja	Bajo	Bajo	Medio

Tabla No. 7. Zonas de riesgo.

La interpretación de los niveles de la escala de riesgo con calificaciones de alto, medio y bajo se puede observar a continuación:

Nivel de Riesgo	Descripción del Riesgo
Alto	Si una situación se evalúa como de alto riesgo, hay una necesidad inminente de tomar medidas correctivas. El activo puede continuar funcionando pero se debe realizar cuanto antes un plan de acción correctiva.
Medio	Si una situación se clasifica como de riesgo medio, las acciones correctivas son necesarias y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
Bajo	Si una situación se clasifica como de riesgo bajo, debe decidirse si las acciones correctivas son requeridas o se acepta el riesgo.

Tabla No. 8. Escalas definidas para el Riesgo.

De acuerdo con el nivel de riesgo identificado para una situación, se asigna una prioridad a las acciones que deben ejecutarse. La prioridad superior se debe dar a las situaciones cuya calificación de riesgo es alta o media.

7.12 Establecimiento de la Aceptabilidad del Riesgo

El objetivo es definir para cuáles riesgos asociados a los activos de los procesos deben ejecutarse acciones de tratamiento. Para lo anterior se manejan dos posibles categorías de riesgo:

Categoría de Riesgo	Criterio	Actividad
Riesgo inaceptable	Nivel de riesgo alto o medio	Se deben aplicar controles de tratamiento del riesgo
Riesgo aceptable	Nivel de riesgo bajo	No se deben aplicar controles de tratamiento del riesgo

Tabla No. 9. Categorías de riesgo.

Para determinar si el riesgo sobre cada uno de los activos, es aceptable o no, se hace un análisis de acuerdo con el nivel de importancia (impacto) y la probabilidad de amenaza a la que se ve expuesto el activo. Debe tenerse en cuenta que el riesgo crece con el impacto y con la probabilidad.

		Impacto		
		Bajo	Medio	Alto
Probabilidad	Alta	Riesgo inaceptable	Riesgo inaceptable	Riesgo inaceptable
	Media	Riesgo aceptable	Riesgo inaceptable	Riesgo inaceptable
	Baja	Riesgo aceptable	Riesgo aceptable	Riesgo inaceptable

Tabla No. 10. Clasificación de las categorías de riesgo.

7.13 Opciones de mitigación del riesgo

Se analizan las opciones de tratamiento de riesgo a aplicar para cada uno de los riesgos considerados como inaceptables. Se busca seleccionar la opción de control más apropiada para la reducción del riesgo a un nivel aceptable por SISTESEG. El tratamiento del riesgo se puede realizar con cualquiera de las siguientes alternativas de control:

Tratamientos del riesgo	Descripción
Asumir el Riesgo	Consiste en aceptar el riesgo potencial y continuar con las actividades asociadas a los procesos de manera normal.
Evitar el Riesgo	Evitar el riesgo mediante la eliminación de su causa. Si se determina, por ejemplo, que la Internet genera riesgos, no utilizarla.
Transferir el Riesgo	Transferir el riesgo mediante la adquisición de pólizas de seguro o entrega del

Tratamientos del riesgo	Descripción
	activo a un tercero que asuma su cuidado y protección.
Mitigar el Riesgo	Implementación de controles físicos, lógicos o administrativos según el activo en consideración. Los controles administrativos son de menor costo.

Tabla No. 11. Opciones de tratamiento del riesgo.

7.14 Plan de tratamiento de riesgos

En esta actividad, se analiza el mapa de riesgos, y teniendo en cuenta los riesgos que se deben mitigar, se construye un plan de tratamiento de riesgos para el corto, mediano y largo plazo dependiendo del nivel de riesgo tal como se muestra en la tabla siguiente:

Nivel de Riesgo	Descripción del Riesgo	Escala de tiempo para implementar
Alto	Si una situación se evalúa como de alto riesgo, hay una necesidad inminente de tomar medidas correctivas. El activo puede continuar funcionando pero se debe realizar cuanto antes un plan de acción correctiva.	Corto plazo
Medio	Si una situación se clasifica como de riesgo medio, las acciones correctivas son necesarias y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.	Mediano plazo
Bajo	Si una situación se clasifica como de riesgo bajo, debe decidirse si las acciones correctivas son requeridas o se acepta el riesgo.	Largo plazo

Tabla No. 12. Plan de tratamiento del riesgo.

7.15 Estructura del documento

1. Objetivo
2. Alcance
3. Glosario de términos utilizados
4. Metodología para el análisis de riesgos
    a. identificar amenazas
    b. identificar vulnerabilidades.
    c. valorar la pérdida financiera (pf)
    d. valorar la pérdida de imagen (pi)
    e. valorar la probabilidad (pr)

f. valorar el riesgo inherente (ri)
g. identificar controles existentes
h. valorar el nivel de exposición (ne)
i. recomendar controles
j. valorar el riesgo residual (rr)

5. Análisis de la información
6. Establecimiento de la aceptabilidad del riesgo
7. Opciones de mitigación del riesgo
8. Plan de tratamiento de riesgos
9. bibliografía

Figura No. 12. Estructura del documento.

8. DESARROLLAR ESTRATEGIAS DE RECUPERACIÓN

Una estrategia de recuperación es un mecanismo que permite garantizar la continuidad de las operaciones de TI frente a un desastre, emergencia o una interrupción mayor. Son consideradas

como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para mitigar la probabilidad de ocurrencia y el impacto de la interrupción.

Para definir las estrategias de continuidad posibles o viables, de manera efectiva y eficiente, se debe contar con un entendimiento sobre los siguientes aspectos:

1. Resultados del Análisis de Impacto al Negocio (BIA).
2. Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
3. Activos críticos de TI a soportar
4. Porcentaje aceptable de degradación de la operación del proceso o sistema.
5. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
6. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos críticos de TI asociados a los procesos.
7. Amenazas posibles a los activos críticos de TI.
8. Vulnerabilidades existentes en los activos críticos de TI.
9. Costos asociados a sitios alternos, equipos, comunicaciones, personal, entre otros.

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios de TI de SISTESEG, considerando los resultados del BIA, la evaluación de riesgos y complementado lo anterior, con la realización de un análisis cuantitativo de los elementos requeridos para la recuperación.

En la Figura No. 13, se relacionan las actividades complementarias a desarrollar en la fase de Desarrollo de Estrategias de Recuperación:

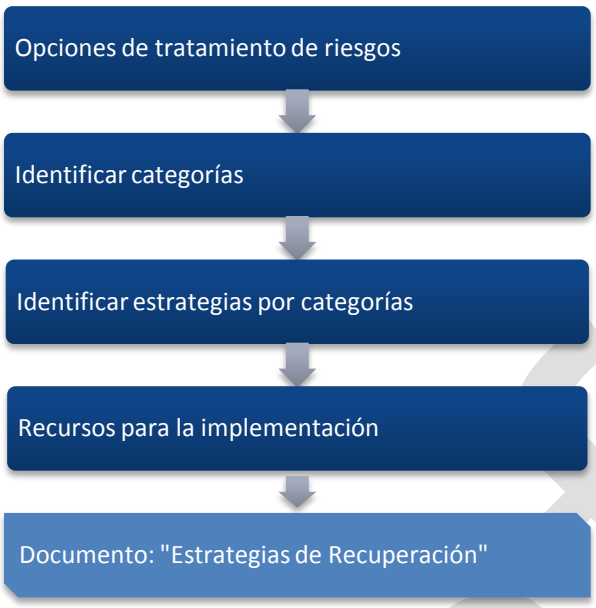

Figura No. 13. Actividades en estrategias de recuperación.

A continuación, se describen cada una de estas actividades.

8.1 Opciones de tratamiento para los riesgos

Se determina cuáles opciones de tratamiento (evitar, transferir, aceptar, atomizar, mitigar, reducir) son aplicables a los riesgos sobre los activos de TI de SISTESEG con base en el Plan de Tratamiento de riesgos de la fase de Análisis de Riesgos. También es importante considerar el costo estimado de la implementación de estos riesgos.

8.2 Identificar categorías de estrategias de mitigación

Se establecen los tipos o clases de estrategias para facilitar la comprensión de la solución total y la evaluación del grado de su cobertura, puede mencionarse la existencia de estrategias tecnológicas (sobre hardware, software, datos, comunicaciones)

8.3 Identificar estrategias de mitigación por categoría

Se formulan controles para cada una de las categorías establecidas, con el propósito de mitigar las distintas consecuencias de un desastre o catástrofe.

Las estrategias de mitigación requieren de la implementación de controles tanto tecnológicos como no tecnológicos. Estos controles buscan por un lado mitigar el impacto de la ocurrencia de un desastre y por el otro reducir la probabilidad de esta ocurrencia. La implementación de las estrategias de mitigación puede ir en paralelo con la implementación de las estrategias de recuperación o continuidad.

Los controles recomendados en la fase de Análsis de Riesgos que hacen parte de la estrategia de mitigación se pueden agrupar en las siguientes categorías:

1. Controles físicos.
2. Controles lógicos.
3. Controles administrativos.

A la implementación de cada uno de estos controles se encuentran asociadas actividades, las cuales se deben realizar e implementar antes de la ocurrencia de un desastre. Estos controles fueron expuestos en el documento de riesgos para los activos críticos de cada sistema o componente de TI.

En lo que sigue de este capítulo nos concentraremos en cuantificar los controles orientados a mitigar el impacto de una interrupción de los activos que soportan los sistemas críticos seleccionados. Para ello consideraremos: tiempos, estrategias, recursos, procesos, RTO's, RPO´s, factores de riesgo y costo de las estrategias.

Una vez definidos los activos críticos del sistema, se debe proceder a realizar un análisis de impacto identificando qué sucede si uno de estos activos permanece por fuera una

determinada cantidad de tiempo. Se busca de esta manera estimar el tiempo máximo que estando el sistema interrumpido pondría en riesgo la continuidad en el tiempo de la entidad.

Para calcular este intervalo de tiempo no solamente se deben considerar los costos asociados de la interrupción del servicio, sino que también se deben considerar los costos asociados a la estrategia de recuperación, la cual entre más corta sea el tiempo que se establezca de recuperación mayor será el valor monetario de su implementación.

El punto óptimo de recuperación se determina considerando el costo del sistema no operativo calculado en diferentes intervalos de tiempo, contra el costo de los recursos requeridos para recuperar el sistema en diferentes tiempos, tal como se observa en la Figura No. 14. En el caso de SISTESEG los tiempos de recuperación fueron estimados con base en entrevistas, acuerdos de servicios que se tienen con algunos clientes, y en general con los impactos asociados a una interrupción.

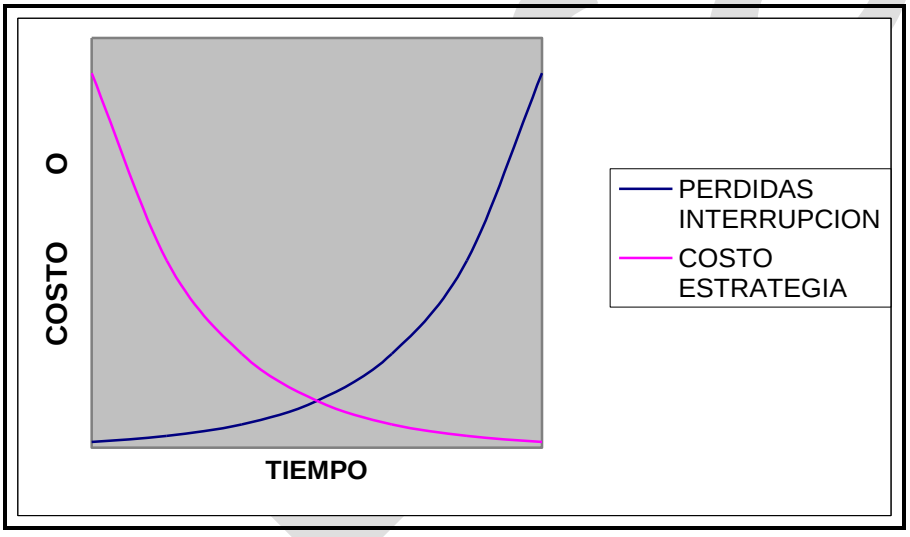

Figura No. 14. Relación costo de la recuperación y el tiempo para recuperarse.

Las estrategias de recuperación según su costo y tiempo de activación se pueden clasificar según la Tabla No. 13.

Sitio	Costo	Hardware	Telecomunicaciones	Tiempo	Localización
Sitio en frío	Bajo	No	Ninguno	Largo	Fijo
Sitio preparado (hot site)	Medio	Completo	Completo	Corto	Fijo
Sitio Móvil	Alto	Variable	Variable	Variable	No fijo
Espejo (Mirror)	Muy Alto	Completo	Completo	Ninguno	Fijo
Soporte datacenter	Medio	Por demanda	Completo	Corto	Fijo

Tabla No. 13. Opciones de tratamiento del riesgo.

Así pues, entre las estrategias de recuperación encontramos las siguientes:

Sitio en frío: consiste típicamente en una facilidad con adecuado espacio e infraestructura para soportar los sistemas tecnológicos. No contiene dispositivos tecnológicos tales como teléfonos, computadores, redes o servidores. De todas las estrategias ésta es la menos costosa pero la que toma más tiempo para que quede operativa y funcionando. Este sitio se podría comprar o también ser un sitio en arriendo.

Hot Sites (sitio preparado): Este tipo de Estrategias está completamente equipada con equipos de oficina y contiene hardware, software, redes y energía. Es mantenido operacional a la espera de recibir las personas que harían uso de sus servicios. Las personas de mantenimiento del sitio empiezan a preparar su operación tan pronto la emergencia es declarada.

Sitio móvil: Este tipo de estrategias está parcialmente equipada con equipos de oficina y contiene parte del hardware, software, redes y energía. Es mantenido operacional a la espera de recibir la orden de trasladarse hacia el sitio en donde se hará la recuperación. Este sitio móvil podría tener también computadores y escritorios para un grupo de trabajo. Esta opción aunque se menciona como una posibilidad hasta el momento no se tiene información que su servicio sea prestado aquí en la ciudad de Bogotá.

Sitio espejo (mirror site): Este tipo de Estrategias está totalmente soportada con equipos de oficina y contiene hardware, software, información, redes y energía. El concepto fundamental

sobre esta estrategia es que es idéntica al sitio principal, desde el punto de vista funcional y en un intervalo muy pequeño de tiempo llegará a estar completamente operativa, este intervalo de tiempo podría estar en el rango de los segundos. Esta opción es la que se ha considerado para SISTESEG en este documento.

Soporte de Datacenter: El servicio de datacenter podría complementar algunas de las estrategias anteriores ya que algunos servicios críticos tales como bases de datos, servidores, aplicaciones, servidores sistema de telefonía, podrían tenerse en un datacenter bajo la modalidad de arriendo de los servidores o del espacio físico para colocarlos y en caso de necesitarse su funcionalidad, se procedería a notificar al servicio de datacenter para que empiecen con las actividades requeridas para que el sistema esté operativo según lo estipulado en el acuerdo de servicio. Este datacenter debería estar retirado una distancia de 30 Km para no compartir los mismos riesgos que el sitio principal.

Por último, las estrategias de recuperación según el tiempo que demore su activación deben dar respuesta a los requerimientos de recuperación de cada uno de los procesos críticos de la entidad. Por ejemplo, dentro de las alternativas propuestas el sitio espejo (mirror site) es la que se utilizaría para procesos con un tiempo de recuperación muy bajo, pero a su vez posee el mayor costo de todas las estrategias analizadas.

El Coordinador del Plan de Contingencia debe asegurar que la estrategia escogida pueda ser implementada efectivamente contando con el personal disponible y los recursos financieros asignados. El costo de las diferentes opciones, tales como sitio alterno, reemplazo de equipos y almacenamiento externo deben ser sopesadas contra las limitaciones de presupuesto y los costos asociados y relacionados con cada una de estas iniciativas. La Tabla No. 14 ofrece un formato para ayudar en la realización de esta labor.

Costos		Proveedor	Hardware	Software	Transporte	Mano de obra	Pruebas	Insumos
Sitio Alterno	Cold site							
	Warm site							
	Hot site							
	Mobile site							
	Mirror site							
Almacenamiento externo	Comercial							
	Interno							
Reemplazo de equipo	SLA							
	Almacenamiento							
	En existencia							

Tabla No. 14. Formato para presupuesto de recuperación.

8.4 Recursos necesarios para la implementación de las estrategias

Según las necesidades planteadas por los requerimientos del Plan de Contingencia, se deben identificar los recursos que deben soportar la estrategia y de esta manera garantizar la continuidad de las operaciones de TI. Algunos ejemplos de recursos son:

- **Infraestructura de telecomunicaciones:** Dispositivos de comunicación para el personal requeridos durante la emergencia, canales de telecomunicaciones y dispositivos de comunicación de voz y datos.
- **Infraestructura tecnológica:** Hardware, software, proveedores, licencias de software, versiones de las soluciones, entre otros. El Plan de Contingencia debe complementar a la estrategia del BCP en lo referente a TI.
- **Personal:** Número de personas que deben apoyar la estrategia de contingencia y su respectivo perfil adecuado a las necesidades, para que puedan cumplir con las labores designadas de manera óptima. En caso de un desastre se debe contar con personal adicional, los que deberían poder reemplazar al personal de operación normal sin el mayor contratiempo y con la misma efectividad.

9. DESARROLLO DEL PLAN DE CONTINGENCIAS

Para cada una de las estrategias de mitigación y reducción establecidas deben identificarse los métodos, plazos, personas, recursos y tareas necesarias para implementarlas. Igualmente, deben establecerse las estructuras organizacionales, los perfiles de los cargos y los procedimientos, que darán sostenibilidad al Plan de Contingencia.

En la Figura 15, se relacionan las actividades a desarrollar, las entradas requeridas y los productos que se generan en la fase de implementación del Plan de Contingencia.

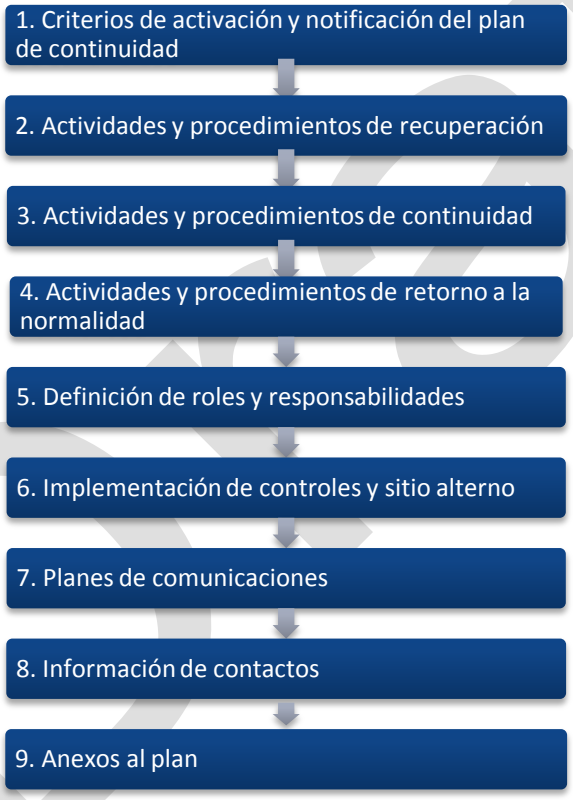

Figura No. 15. Implementación del Plan.

A continuación se describen cada una de estas actividades:

1. Criterios de activación y notificación del plan de continuidad:

2. Actividades y procedimientos de recuperación:
3. Actividades y procedimientos de continuidad:
4. Actividades y procedimientos de retorno a la normalidad:
5. Definición de roles y responsabilidades:
6. Implementación de controles y sitio alterno:
7. Planes de comunicaciones:
8. Información de contactos:
9. Anexos al plan:

9.1 Criterios de activación y notificación del PCN

Los criterios para la activación y notificación del PCN deben ser definidos de manera precisa y clara en la fase de implementación del Plan. Se busca que no por cualquier incidente menor se tenga que proceder a realizar la activación del PCN y asumir de esta manera los riesgos que esto conlleva. Entre otras definiciones y actividades se tienen:

1. Definir qué es un desastre mayor
2. Definir qué es un desastre intermedio
3. Definir qué es un desastre menor
4. Activar los diferentes equipos que conforman el Plan
5. Definir los disparadores (triggers, por su denominación del inglés)
6. Definir los disparadores para la transición entre fases

Figura No. 16. Activación del Plan.

Con el fin de determinar la activación del Plan de Contingencia después de una emergencia, es importante evaluar la naturaleza y la extensión del daño al sistema o componente. La evaluación del

daño debe ser realizada a la mayor brevedad, considerando la seguridad del personal. El equipo de evaluación de daños debe considerar los siguientes aspectos (ver anexo 1):

1. Causa de la emergencia, desastre o interrupción
2. Potencial para otras consecuencias o daños colaterales
3. Área afectada
4. Estado de los edificios, plantas, oficinas, energía, aire acondicionado, entre otros
5. Inventarios de estado de equipos de TI (funcional, parcialmente funcional, destruido)
6. Tipo de daños a los equipos de TI (incendio, agua, calor, impacto físico, entre otros)
7. Listado de equipos para ser reemplazado
8. Tiempo estimado para que retorne el servicio

El Plan de Contingencia debe ser activado cuando el equipo de evaluación de daños ha indicado que uno o más criterios de activación han sido cumplidos. Si el criterio ha sido cumplido el Coordinador del Plan de Contingencia o respaldo de él, deberá activar el Plan. Los criterios de activación deben estar basado en:

1. Seguridad del personal o extensión del daño
2. Cantidad de activos afectados de TI
3. Criticidad de los activos afectados
4. Tiempo estimado de duración para retornar el servicio

Por otra parte, la estrategia de notificación debe definir procedimientos para seguirse en caso de un desastre o interrupción para que los diferentes equipos y personas, que conforman el Plan, puedan ser contactados. Un método común de notificación es denominado el árbol de llamadas. Esta técnica involucra asignar tareas de notificación a individuos específicos, que son a su vez responsables de contactar otras personas, tal como se muestra a continuación.

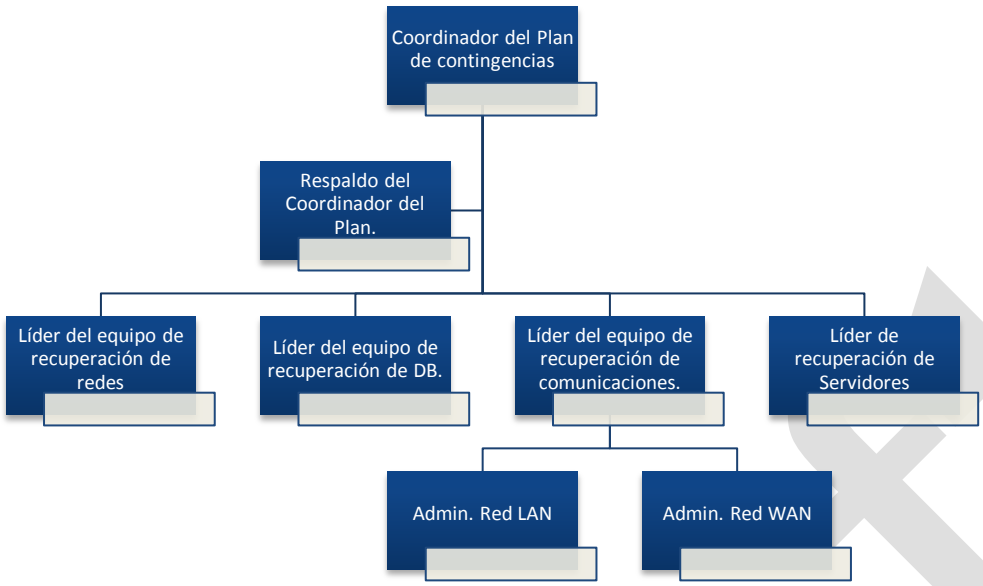

Figura No. 17. Ejemplo de árbol de llamadas.

9.2 Actividades y procedimientos de recuperación

Las actividades y procedimientos de recuperación corresponden a la definición detallada y precisa de los documentos que servirán de apoyo para el proceso de recuperación. Las actividades de recuperación forman parte de las cuatro actividades principales que deben conducir al retorno a la operación normal una vez sucedido un evento que pueda interrumpir de manera severa las operaciones de SISTESEG.

Las actividades relacionadas con la recuperación corresponden al trabajo que se debe realizar una vez ha ocurrido el desastre o interrupción. En esta fase se asume que el equipo de evaluación de daños ha realizado su labor para contener y detener el desastre y se ha tomado la decisión de activar el Plan dado que se cumplieron los criterios definidos para ello.

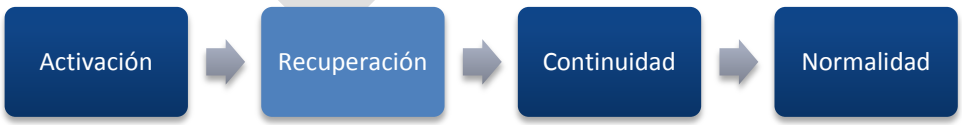

Figura No. 18. Actividades de recuperación.

9.3 Actividades y procedimientos de continuidad

Las actividades y procedimientos de continuidad se llevan a cabo una vez completada la actividad anterior de recuperación. Estas actividades comprenden los pasos a seguir con el fin de regresar el negocio a su operación usual. Normalmente en esta actividad se consideran los pasos a seguir para retornar de sitio alterno a sitio principal.

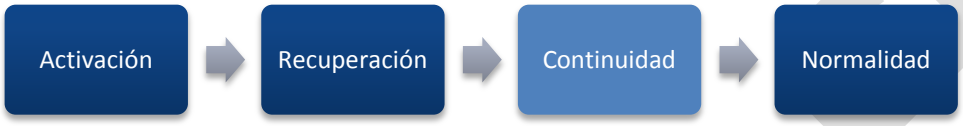

Figura No. 19. Actividades de continuidad.

9.4 Actividades y procedimientos de retorno a la normalidad

Esta fase puede existir o no dependiendo de la criticidad del desastre ocurrido y teniendo en cuenta qué tanta destrucción tanto material como humana se generó. Es posible que debido a la severidad de la situación el retorno a la normalidad no pueda ocurrir. Es probable que el edificio tenga que ser reconstruido o adquirido, con la cual esta actividad se concentrará en temas de adecuación e instalación al nuevo sitio principal y otra serie de ajustes y cambios. Así pues, esta fase debe ser considerada cuando el desastre produzca tantos cambios en la organización que realmente nunca se va a llegar a una operación igual a la que teníamos antes del desastre.

Figura No. 20. Regreso a la normalidad.

9.5 Definición de roles y responsabilidades

En esta actividad deben establecerse las estructuras organizacionales, los perfiles de los cargos y los procedimientos asociados que darán sostenibilidad a la continuidad del negocio. La definición de roles

y responsabilidades es uno de los aspectos más importantes del Plan de Continuidad del Negocio, porque es aquí en donde se determinan cada una de las actividades a ejecutar antes, durante y después del desastre. Sin estos recursos no sería posible hacerlo funcionar. Entre los roles que se considerarán durante la ejecución del proyecto están:

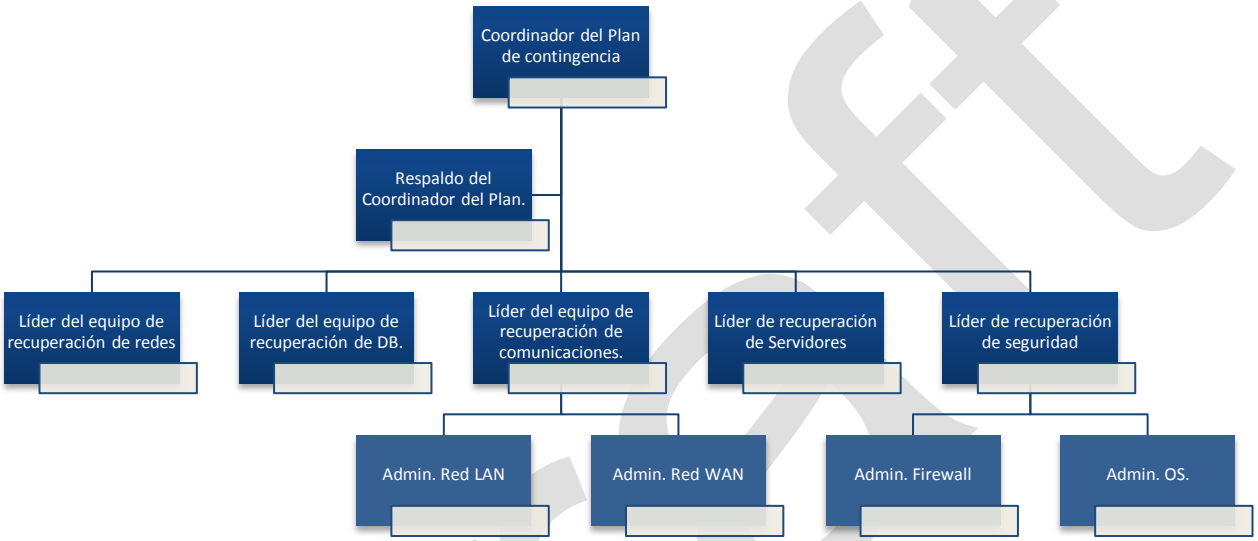

Figura No. 21. Ejemplo de una estructura para el Plan.

9.6 Implementación de controles y sitio alterno.

Esta fase tiene como objetivo primordial definir las tareas y asignar recursos con el fin de implementar las estrategias de mitigación. Es recomendable en esta fase contar con una metodología efectiva para la gestión de proyectos con el fin de lograr definir de manera precisa los recursos requeridos, los tiempos de adquisición, instalación, prueba y afinamiento de los controles definidos. Por ejemplo, en esta fase se puede decidir la adquisición y puesta en funcionamiento de un generador de potencia eléctrica, para ello se debe realizar una invitación a diferentes proveedores, realizar la selección del proveedor y marca del equipo, instalar, configurar, probar y llevarlo a producción.

Uno de los controles a implementar y en que normalmente y tradicionalmente se ha hecho una gran inversión es el tema de sitio alterno. Para esto se recomienda seguir los siguientes pasos:

1. Definir criterios de selección tecnológicos
2. Definir criterios de selección funcionales
3. Definir ubicaciones
4. Realizar análisis financieros de la inversión
5. Definir términos contractuales
6. Definir criterios de selección de proveedores
7. Proceder a la adquisición
8. Realizar pruebas

Figura No. 22. Adquisición de sitio alterno.

9.7 Planes de comunicaciones

Los planes de comunicación corresponden a las actividades que se realizan durante un desastre para mantener a ciertos grupos de personas informados sobre el desastre ocurrido, su alcance, sus consecuencias, y estrategias de recuperación previamente definidas en el corto, mediano y largo plazo, con el fin de generar un parte de tranquilidad y de esta manera expresar el respeto a la vida, la urgencia y la preparación con que se responde ante este tipo situaciones. Entre los grupos sobre los que se elaboran mensajes específicos están:

1. Empleados
2. Integrantes del PCN

3. Clientes
4. Proveedores
5. Junta directiva
6. Comunidad de Popayán
7. Público en general

9.8 Información de contactos

Una parte fundamental del PCN, es contar con una lista de contactos para ser utilizado en caso de presentarse la activación del PCN. Esta lista debe contener al menos:

1. Integrantes del PCN
2. Empleados requeridos
3. Directivos
4. Proveedores
5. Clientes
6. Números de emergencia (policía, bomberos, energía, empresas de recuperación, entre otros)

9.9 Anexos al plan

En este punto se debe considerar qué información adicional es necesario adjuntar al plan con el fin de hacerlo auto-contenido, es decir, que esta información adicional sea relevante, lo complemente y sea útil en caso de la utilización del plan.

Por ejemplo, diagramas de red, información técnica de servidores, listado de activos críticos, políticas, procedimientos, estándares de configuración, pólizas de seguros, formatos, listas de contactos, entre otros pueden ser parte de los anexos del plan, y en caso de necesitarse su actualización no será necesario actualizar todo el plan.

10. ENTRENAMIENTO

El entrenamiento incluye, entre otros aspectos, el adiestramiento al personal en sus roles y responsabilidades relacionadas con el plan, así como el entrenamiento en habilidades específicas que necesitarán para llevar a cabo sus roles efectivamente. El entrenamiento, como tal, es un proceso que involucra el aprendizaje de conceptos y términos utilizados en

procesos de continuidad del negocio. El entrenamiento también cubrirá el uso adecuado y efectivo del Plan. En la figura No. 23, se observa cada una de las actividades que hacen parte del entrenamiento, que comprenden su desarrollo, sensibilización y monitoreo del Plan.

10.1 Desarrollo del plan de entrenamiento

En la fase de desarrollo del plan de entrenamiento se busca capacitar a los coordinadores y líderes de equipo del Plan de Contingencia en lo referente a la gestión y ejecución del Plan. También se darán a conocer las responsabilidades asociadas a cada uno de los roles definidos en el Plan. Para lograr lo anteriormente mencionado, se debe crear un documento denominado Plan de Entrenamiento, el que contiene las actividades a realizar para lograr desarrollar un Plan de Entrenamiento adecuado sobre el Plan de Contingencia de SISTESEG.

Figura No. 23. Actividades del entrenamiento.

Para realizar el entrenamiento se pueden utilizar múltiples formatos, entre ellos:

- Presentación a grupos.
- Conferencias telefónicas.
- Documentos publicados en la Intranet.
- Clases magistrales.
- Conferencias.
- Talleres.
- DVD, CD's con información relevante.
- WEB based training.

- Videoconferencia.

Adicionalmente, cada uno de los coordinadores y líderes de equipo del PCN deben saber cómo y cuándo activar el plan y posteriormente, notificar, gestionar y dirigir a los miembros de su equipo. Para esto, ellos necesitan:

- **Usar el plan de forma efectiva**: esta es la parte más básica del entrenamiento. La función del entrenamiento es familiarizar a las personas con los procesos y elementos del plan y adicionalmente, reforzar los conocimientos básicos en lo referente a las funciones del Plan.
- **Comprender los roles y las responsabilidades, tanto de cada miembro como del equipo en general**: al tener un conocimiento de todas las responsabilidades del equipo, el líder del equipo tendrá mayor control sobre las actividades que se desarrollan en el equipo, para que todo transcurra en orden en una situación de crisis. Hay que tener en cuenta, que los miembros del equipo son muy efectivos si el líder del equipo confía en ellos y a su vez, es una persona realmente competente.
- **Notificar, reunir y dirigir a sus miembros de equipo**: las reuniones constantes del líder (coordinador) con sus miembros del equipo son importantes para determinar y recordar los roles y responsabilidades que posee cada miembro del equipo en caso de que ocurra un incidente o desastre. Además estas actividades mantienen actualizados a todos los miembros del equipo sobre las actividades orientadas a asegurar la continuidad del negocio.
- **Comunicaciones:** El realizar un proceso simulado de comunicación en donde las herramientas de comunicación como el teléfono, e-mail u otros dispositivos y servicios electrónicos se asuma que no están en funcionamiento, es un aspecto importante de la futura activación del Plan. Para realizar esta simulación se requiere apoyarse en listas de comprobación o listas de verificación, árboles de llamada, copias del plan, resúmenes, medios alternos de comunicación y ejercicios de campo.

A su vez, cada uno de los integrantes de los equipos deben recibir entrenamiento en los siguientes aspectos:

1. Propósito del plan.
2. Alcance del Plan (procesos involucrados)
3. Objetivos del Plan.
4. Coordinación y comunicación con el equipo.
5. Estrategias de recuperación.
6. Metodología de análisis de riesgos.
7. Controles existentes.
8. Procedimientos y formatos a utilizar.
9. Requerimientos de seguridad del Plan.
10. Procesos específicos de los equipos (como notificación, activación, recuperación y restauración).
11. Responsabilidades individuales (como notificación, activación, recuperación y restauración).

10.2 Sensibilización en el Plan de Contingencia.

El propósito de la sensibilización sobre el Plan es recalcar la importancia de lo que este Plan representa y los beneficios ofrecidos en caso de presentarse un desastre que ponga en riesgo la vida de los empleados de SISTESEG y los procesos que soportan su funcionamiento. Se busca de esta manera mediante el uso de herramientas educativas que los empleados conozcan los beneficios que se tienen al contar con un Plan preestablecido para el manejo de desastres y entre ellos sobresalen la preservación de la vida tanto de los empleados de SISTESEG como de la comunidad. Por otro lado, se busca crear una cultura adecuada de la gestión del riesgo a lo largo de toda la organización con el fin de que se pueda reaccionar a tiempo ante ciertas amenazas y que esta reacción sea lo más organizada y efectiva en la medida de lo posible y cumplan con los objetivos y tiempos de recuperación.

La sensibilización crea en el personal de SISTESEG las habilidades para la detección oportuna de amenazas y vulnerabilidades asociados a los procesos y les ayuda a reconocer la necesidad de proteger los datos, las personas, la información, los medios utilizados para su procesamiento y demás herramientas empleadas en las labores diarias. Las personas, al integrar estas experiencias en sus actitudes y comportamiento diario, generan dentro de la organización un cambio cultural. La sensibilización en la continuidad del negocio sienta las bases para lograr una cultura en la gestión del riesgo al generar la motivación necesaria, garantizando así, que el proceso de aprendizaje sea más efectivo, es decir, se pueda reaccionar de manera controlada y efectiva ante amenazas que afecten la continuidad de los procesos críticos de SISTESEG.

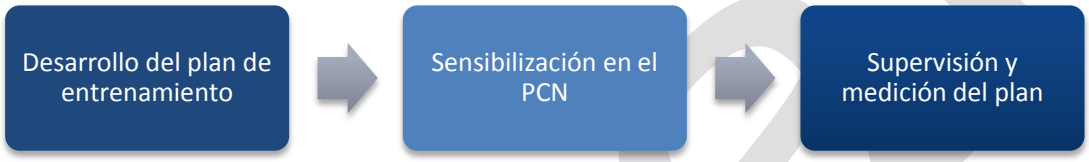

Figura No. 24. Actividades del entrenamiento.

Dentro de las estrategias complementarias al desarrollo de la sensibilización se recomiendan las siguientes:

1. Creación de un *slogan* que identifique la campaña de sensibilización y sea fácil de recordar.
2. Afiches que muestren el impacto de ciertas amenazas o el impacto al no contar con una política de gestión de riesgos.
3. Mensajes escritos en la pantalla en el momento de hacer ingreso por parte de los empleados a servicios o aplicaciones.
4. Presentaciones realizadas por expertos que muestren desastres ocurridos en Colombia o en otros países y su impacto en la continuidad del negocio.
5. Películas (videos) que muestren desastres ocurridos e investiguen las causas del mismo.

6. Envío de mensajes de manera periódica que refuercen las políticas o procedimientos de seguridad y manejo de riesgos.
7. Asistencia a seminarios, talleres y cursos tanto nacionales o internacionales sobre gestión de riesgos.
8. Suscripción a revistas sobre el tema de continuidad del negocio por parte del equipo del Plan. Entre los organismos que recomendados están el BCI (Business Continuity Institute) y el DRI (Disaster Recovery Institute).
9. Contar con acceso a páginas en Internet o listas de correo sobre temas de:
    - Desastres
    - Noticias
    - Clima
    - Eventos geológicos
    - Gobierno
    - Emergencias

10.3 Supervisión y mediciones del plan

Por último, el plan de entrenamiento y sensibilización debe ser supervisado con el fin de revisar su efectividad. También se deben hacer mediciones sobre qué tan bien están capacitados sobre los aspectos del Plan las personas que interactúan con él, ya sea de manera directa o indirecta. Para lo anterior se puede hacer uso de herramientas automatizadas que cuenten con esquemas de aprendizaje y de evaluación. Tanto los resultados del monitoreo y de las mediciones deben ser revisadas por el Coordinador del Plan, con el fin de que él tenga información sobre los avances hechos tanto en el entrenamiento como en el proceso de sensibilización y pueda generar recomendaciones para la posterior mejora de estos procesos.

Figura No. 25. Actividades del entrenamiento.

11. PRUEBAS

La efectividad del Plan de Contingencia en situaciones de desastre se puede comprobar mediante un plan de prueba que permita revisar dicha efectividad antes de enfrentarse a una situación real[3]. La fase de pruebas debe considerar las actividades estipuladas en el documento de roles y responsabilidades presentes en el Plan. Estas actividades se deben probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera teniendo en cuenta no poner en riesgo la operación real como consecuencia de esta prueba. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis según su rol. Estas pruebas deben estar dirigidas por el Coordinador del PCN y deben realizarse mínimo una vez al año o antes si existe un cambio sustancial en las condiciones del Plan, según lo sugerido por las mejores prácticas y recomendaciones internacionales. También es importante anotar que es posible realizar pruebas ya no simuladas, sino, que los activos que soportan los procesos se pongan fuera de servicio y de esta manera contar con una prueba más real, sin embargo, este tipo de pruebas pueden convertirse en un desastre y por eso es importante hacer siempre antes una planeación muy detallada de este tipo de pruebas y analizar sus riesgos inherentes.

En la figura No. 26, se muestran las actividades que se deben seguir para realizar la fase de pruebas.

[3] Se tiene información de que el 80% de los planes que se prueban muestran serias debilidades.

Figura No. 26. Actividades en el proceso de pruebas.

A continuación se explican detalladamente cada una de estas actividades.

11.1 Planear la Prueba

Esta actividad implica una planeación detallada de las actividades a realizar. La planeación de las pruebas es un factor crítico ya que de ello depende que las pruebas no afecten la operación normal del sistema. Como salida de esta actividad se tendrá un Plan de Pruebas debidamente documentado y aprobado.

Las actividades concretas que deben realizarse son:

- Definir y documentar el alcance de la prueba.
- Revisar los roles y responsabilidades propios para la ejecución de la prueba.
- Elaborar formatos requeridos para la prueba
    - Formato de preparación de la prueba
    - Formato de inventario requerido
    - Formato de criterios de aceptación e evaluación
    - Formato de registro
    - Formato de lista de distribución
- Cronograma de prueba (definir fecha y hora tentativa)
- Definir personal que estará involucrado en las pruebas
- Recursos requeridos para la prueba (tecnológicos y logísticos)
- Definir y documentar criterios de aceptación de la prueba
- Definir y documentar criterios de evaluación de la prueba
- Elaborar listas de verificación.
- Elaborar procedimientos para la prueba que incluyan mínimo:
    - Objetivo
    - Alcance

    - Responsables
    - Audiencia
    - Políticas y lineamientos
    - Glosario de términos
    - Flujogramas
- Asignación de presupuestos.
- Reuniones de aclaración.
- Estrategia de notificación para los integrantes del Plan, empleados y clientes.
- Conseguir permisos y aprobaciones requeridas.
- Generar documento de Plan de Pruebas.
- Aprobar documento de Plan de Pruebas por parte del Coordinador del PCN.

11.2 Definir el Alcance de la Prueba

El alcance de la prueba se debe determinar con base en los recursos que se cuentan para su posible realización y el porcentaje de afectación que se puede infringir a los procesos. Se debe determinar también el efecto que tengan las pruebas sobre los procesos seleccionados como parte del PCN de SISTESEG y los respectivos subsistemas que lo componen. Una vez determinado el alcance se debe proceder a contar con la aprobación por parte del Coordinador del PCN y los respectivos dueños de los procesos involucrados. Entre los aspectos a considerar como parte del alcance están:

1. Procesos involucrados
2. Activos involucrados
3. Personal requerido
4. Instalaciones comprometidas
5. Clientes afectados
6. Gastos requeridos
7. Tiempo que tomará la prueba

8. Tipo de prueba a realizar
    a. Simulación
    b. Recorrido
    c. Prueba de interrupción completa[4]
9. Actualizar documento de Plan de Pruebas.

11.3 Procedimientos detallados en la prueba del PCN

En la tabla 15, se muestra un ejemplo de un procedimiento sugerido y detallado para la prueba tipo "recorrido[5]" con el fin de comprobar la efectividad del PCN:

Número de actividad	Descripción de la actividad
1	El Coordinador del PCN debe reunir al Coordinador de la Gestión Administrativa, a los Líderes de Equipos y a sus respectivos miembros.
2	Una vez este equipo reunido se debe entregar copias impresas del PCN a cada uno de los integrantes del equipo. Los integrantes del equipo deben hacer una lectura de 30 minutos del documento PCN con el fin de entenderlo en su totalidad y en caso de dudas se deben plantear a todo el equipo para llegar a una posible respuesta o consenso.
3	El Coordinador del PCN debe leer paso por paso los roles y responsabilidades de cada equipo. Los integrantes del equipo deben escuchar atentamente esta lectura y tratar de prever que circunstancias pudieran afectar el desarrollo de estas actividades y tomar nota de ellas para una posterior discusión.
4	Realizar una discusión de aproximadamente una hora sobre los temas que los integrantes de los equipos consideraron como posibles fallas a las actividades anteriormente leídas.
5	El Coordinador del PCN debe tratar de llegar a un consenso con los integrantes del Plan sobre las modificaciones que se deberían hacer a las actividades del documento roles y responsabilidades para luego ser implantadas en él.
6	Generar comentarios adicionales sobre los resultados obtenidos después de realizado este ejercicio.
7	Dar por terminado el ejercicio y el Coordinador del PCN generará un acta de la reunión la cual será anexada al documento del PCN y se realizarán en él los cambios consensuados.

Tabla No. 15. Procedimiento de prueba tipo "recorrido".

[4] Este tipo de prueba no es considerada en este documento debido al extremo cuidado que se debe tener al realizarla y su complejidad. Considera interrumpir de manera real los activos que soportan un proceso determinado. En muchos casos este tipo de pruebas se puede convertir en un desastre.

[5] Como su nombre lo indica sólo se hace un recorrido (lectura) por el documento PCN, sus roles y procedimientos.

En la tabla 16, se expone el procedimiento detallado de la prueba tipo "simulación[6]" sugerida con el fin de comprobar la efectividad del PCN:

Número de actividad	Descripción de la actividad
1	El Coordinador del PCN debe reunir en un sitio predeterminado al Coordinador de la Gestión Administrativa, a los Líderes de Equipos y sus respectivos miembros, el cual debe contactar a su vez a sus líderes de equipo y estos a los miembros de los equipos. Una vez reunidos se les entrega copia de los procedimientos pertinentes a cada miembro y líderes de los equipos y se le instruye sobre el alcance y los objetivos de la prueba a realizar.
2	Utilizando la lista de contactos de empleados, en propiedad de Coordinador del PCN se debe proceder a contactarlos. Se debe exigir a estar personas que utilicen los medios a disposición para que su llegada a sus respectivos sitios de operación sea en máximo 30 minutos. Se entiende que la prueba se realiza cuando los empleados no están laborando de manera normal.
3	Proceder a realizar los arreglos para tener los medios de transporte listos para el traslado del personal, en caso de ser requerido.
4	Verificar que permisos de entrada a los sitios de operación alterna hayan sido tramitados.
5	Revisar las condiciones físicas en los sitios preestablecidos para que este personal pueda realizar las labores asociados al proceso respectivo.
6	Revisar que las personas cuenten con equipos, sitio, sillas y medios para realizar sus actividades. Proceder al ingreso del personal al sitio preestablecido para la operación en caso de un desastre.
7	En este punto dar por terminada la prueba, y el Coordinador del PCN debe generar un informe de lo relevante encontrado en esta prueba y debe anexar este documento al PCN y proceder a su actualización.

Tabla No. 16. Procedimiento de prueba tipo "simulación".

11.4 Ejecutar la Prueba

Las pruebas se deben llevar a cabo bajo condiciones cercanas a la realidad y todos los participantes deben colaborar activamente en su realización. Es importante que todas las personas que probablemente participen en caso de ser activado el PCN hagan parte del plan de pruebas y colaboren en revisarlo detalladamente antes, durante y después de la ejecución de estas pruebas.

Para ejecutar las pruebas se deben considerar:

[6] La prueba tipo simulación no comprende afectar ningún activo de los procesos, pero si el contacto y posterior traslado a sitio alterno, junto con el entendimiento de los roles y responsabilidades tanto del equipo del PCN, como de algunos empleados.

- Revisión detallada de roles y responsabilidades.
- Interacción del PCN con el BCP
- Revisión de listas de contactos de proveedores, equipos PCN y empleados.
- Revisión de acuerdos de transporte y adquisiciones.
- Revisión de los árboles de llamada.
- Revisión de los procesos de notificación y activación.
- Revisión de los procedimientos detallados de operación en caso de un desastre.
- Ajustes finales en la fecha y hora.
- Contar con mecanismos para abortar la prueba si ocurre algo inesperado
- Realizar un informe formal de los resultados obtenidos
    - Resumen de eventos
        - Lo que se hizo de manera incorrecta
        - Lo que se hizo de manera correcta
    - Tiempo requeridos
    - Recomendaciones
- Actualizar el PCN
    - Cambios al Plan de Pruebas
    - Cambios al organigrama del Plan
    - Cambios en roles y responsabilidades
    - Cambios a los procedimientos del Plan
    - Cambios a las listas de verificación y formatos

12. AUDITORÍA

La auditoría del Plan es un proceso en el que se revisa el PCN contra requerimientos específicos estandarizados por la industria. La auditoría también es una revisión imparcial del para verificar si él cumple con las necesidades de la organización. Por otro lado, la auditoría debe ser realizada como un proyecto estándar y un plan de auditoría debe ser creado antes de su realización.

En el proceso de auditoría se deben tener en cuenta varios elementos importantes, entre los cuales se encuentran:

- Revisar el BIA y verificar que esté actualizado.
- Revisar la metodología del Análisis de Riesgo.
- Revisar que el análisis de riesgo esté actualizado.
- Asegurarse de que las estrategias de mitigación de riesgos hayan sido implementadas apropiadamente.
- Revisar la efectividad de los controles implementados.
- Revisar el Plan de Pruebas y Entrenamiento.
- Revisar cómo se hace el mantenimiento del Plan.
- Revisar los procesos y documentos de sensibilización.
- Recolectar evidencias sobre las actividades realizadas relacionadas con el PCN dentro de SISTESEG.
- Entrevistar al coordinador del PCN y a otros integrantes de los equipo sobre las actividades que desempeñan dentro del Plan.
- Revisar el documento de resultados de las pruebas.
- Revisar los formatos del PCN que se diligencian, antes, durante y después de un desastre.
- Verificar la efectividad de las herramientas que apoyan el PCN.

- Generar recomendaciones al Plan.
- Presentar informe de auditoría.
- Verificar que en un tiempo de máximo 1 mes las recomendaciones expuestas en el informe de auditoría se hayan implementado.

13. MANTENIMIENTO DEL PLAN

En la fase de mantenimiento del Plan de Contingencia de SISTESEG, se deben tener en cuenta todos los cambios relevantes ocurridos en el entorno del PCN, ya que ellos modifican su alcance y, por lo tanto, deben quedar debidamente incluidos en el documento PCN. En la figura No. 27, se muestran las entradas que pueden ocasionar cambios al PCN, es decir, cuando ocurran cambios regulatorios, en el entorno, tecnológicos, o los generados por el informe de pruebas o auditorías, entre otros. El PCN de SISTESEG deberá ser actualizado una vez al año, o cuando ocurra un cambio significativo en los procesos críticos de la organización.

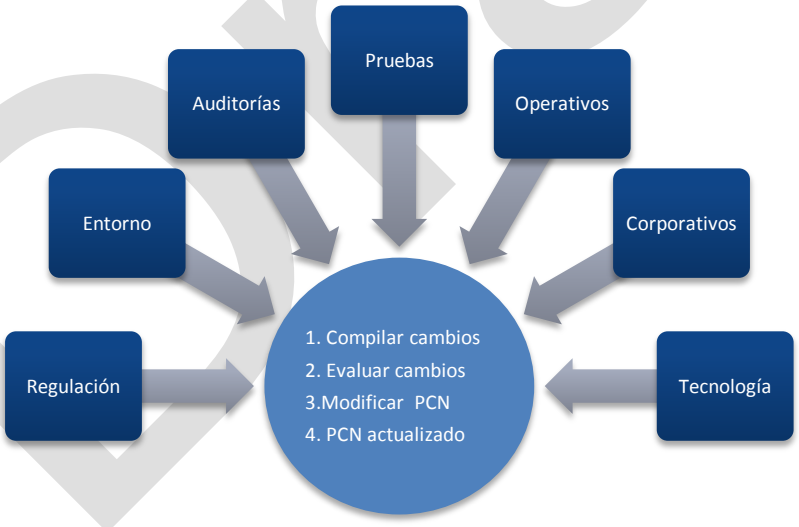

Figura No. 27. Mantenimiento del plan.

ANEXO 1

LISTA DE VERIFICACIÓN PROCEDIMIENTO DE ACTIVACIÓN Y RECUPERACIÓN.

Nota: Generalmente esta lista de verificación se sigue en orden secuencial pero algunas acciones podrían hacerse en paralelo.

Ocurrencia del evento

- Detección incidente
- Reporte incidente
- Respuesta de emergencia

Contactos iniciales a notificar

- Nombre 1
- Nombre 2
- Nombre 3

Nombre	Teléfono del trabajo	Teléfono de la casa	Celular	E-mail

Lista de Contactos de Personal

- **Sitio de reubicación** (en el evento de evacuación)
  - Indicar el punto de encuentre e informarlo
  - Conteo del personal

- **Realice una evaluación preliminar.** Determine:
  - Estado de la emergencia
  - Análisis del incidente
  - Fatalidades y lesiones
  - Áreas afectadas
  - Seguridad

- Acceso al edificio

- **Estado de lo siguiente:**

  - Edificios
  - Energía
  - Servicios públicos
  - HVAC
  - Condiciones ambientales
  - Centro de datos
  - Comunicaciones de voz
  - Comunicaciones de datos

- **Designar el centro de comando** (Dos posibilidades son recomendadas)

  - En el edificio principal (si es habitable)
  - Edificio alterno (Dirección, teléfono y mapa)

- **Realice un informe público de la situación** (si apropiado)
- **Evaluación de daños**

  - Formar el equipo
  - Informe al equipo de daños
  - Evaluar daños
  - Documentar el daño con fotos, documentos y otros.
  - Analizar el daño y su impacto
  - Identificar equipo recuperable

- **Desarrollar un consolidado Plan de Acción**

  - Revisar la estrategia de Recuperación
  - Revisar el estado de las operaciones
  - Evaluar impacto al servicio
  - Desarrollar recomendaciones para la recuperación
  - Revisar los MAO
  - tiempos de recuperación
  - Finalizar recomendaciones
  - Revisar los criterios de la declaración de desastre
  - recomendaciones para la declaración del desastre
  - Realizar un informe a las directivas
  - Obtener aprobación de declaración del desastre y obtener declaración a los medios
  - Decisión sobre el desastre
    - Si Declaración = No
      - Recuperación en proceso con recursos locales
    - Si Declaración = Si
    - Activar PCS
    - Notificar a los Coordinadores de la reubicación según el PC

- Movilizar Equipos del Plan de contingencia
- Informar a los Líderes de Equipo y Coordinadores sobre el evento

Miembros

- Activar personal de soporte (si apropiado)

Por ejemplo:

- Recursos humanos [nombre]
- Finanzas [nombre]
- Legal [nombre]
- Servicios de oficina
- Manejo de medios, registros y documentos
- Distribución
- Medios de transportes y viajes
- Transporte
    - Revisar acuerdos de servicios y activarlos
    - Hacer gestiones adicionales según el contrato
    - Reubicación del personal
- Equipos: Implementar planes de recuperación
- Operación en modo contingencia
- Coordinar acciones de recuperación
    - Reporte de estado
    - Informes periódicos
- Iniciar Procedimiento de restauración (si apropiado)
- Restauración
- Realice un análisis posterior al incidente
    - Revisar registros
    - Documentar lecciones aprendidas
    - Preparar informe