2017

V 1.0

METODOLOGIA: PLAN DE RECUPERACION ANTE DESASTRES (DRP) ISO 27031:2011 (IRBC) e ISO 22301:2012

17/08/2017

CONTROL DOCUMENTAL

Historia

Versión	Autor	Tipo de Revisión	Descripción	Aprobado por	Fecha
1.0	SISTESEG	Creación	Proyecto		

Distribución

Copia	Destinatario	Destino / Dirección
Original	SISTESEG	
Copia	SISTESEG	

Referencias

Ref.	Documento o ítem referenciado

Control de Acceso

Sección	Disponibilidad
Todo	

TABLA DE CONTENIDO

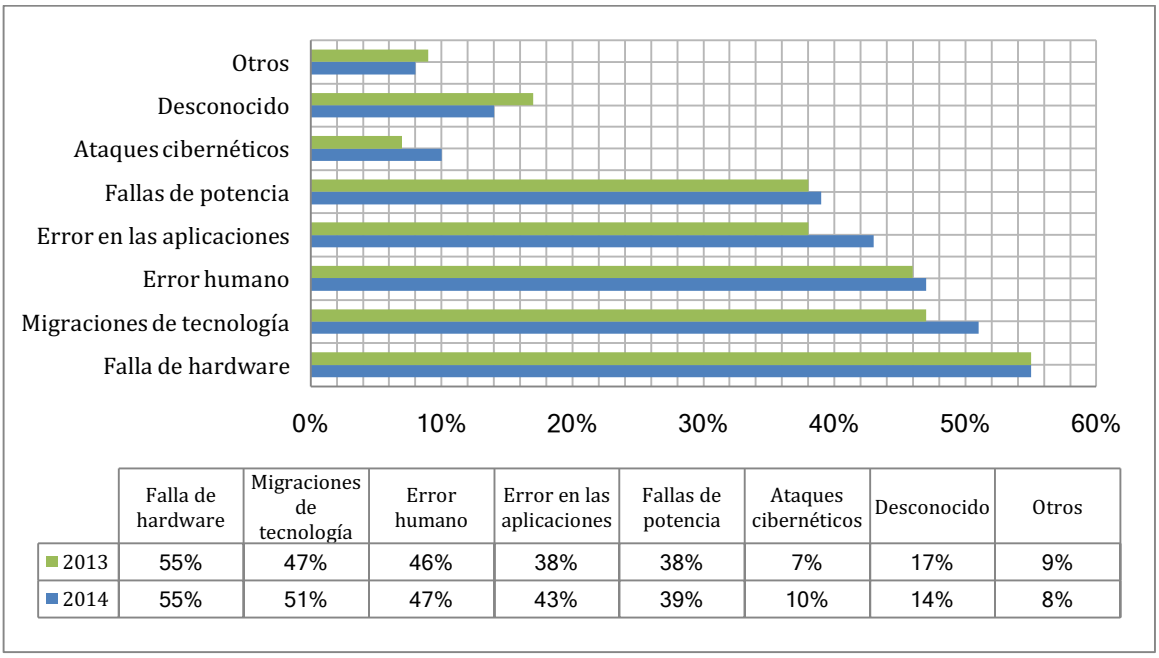
1 PLAN DE RECUPERACIÓN ANTE DESASTRES

1.1 ENTENDIMIENTO DE LAS NECESIDADES

En los últimos años, algunas entidades a lo largo del territorio nacional, han concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante incidentes de diversas categorías y diferentes niveles de impacto. Estos factores, junto con una legislación cada vez más exigente, en lo relacionado a la confiabilidad y seguridad en la prestación de estos productos y servicios, hacen necesario en la actualidad que se cuente con una DRP (Disaster Recovery Plan) (ISO 27031:2011, ISO 22301:2012), con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, de la disponibilidad de los procesos del negocio, de la información (ISO 27001:2013) y del conocimiento, de la tecnología, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves y el ciberterrorismo[1], han mostrado la necesidad de incorporar nuevas amenazas en el DRP con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información, por dos años consecutivos, ha permanecido en el primer lugar de acuerdo al 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%.

[1] EL BCI Horizon Scan, evaluó 760 organizaciones a nivel mundial y comprobó que el (82%) de los líderes de continuidad temen por un ciberataque inminente. Estos ataques pueden generar unas pérdidas de alrededor de $7.6 millones de dólares por empresa y con un crecimiento anual de 10.4% en el número de estos ataques.



	Falla de hardware	Migraciones de tecnología	Error humano	Error en las aplicaciones	Fallas de potencia	Ataques cibernéticos	Desconocido	Otros
2013	55%	47%	46%	38%	38%	7%	17%	9%
2014	55%	51%	47%	43%	39%	10%	14%	8%

Figura No. 1. Causas de activación del BCP/DRP en porcentaje (fuente: Continuity Software).

Se plantea la necesidad de desarrollar un DRP que permita dar continuidad a sus productos y servicios críticos en caso de una interrupción los inhabilite. Los productos y servicios dependen de Software, Hardware, Comunicaciones, Servicios, Datos, Personas, Equipos Auxiliares, Instalaciones, los cuales de una forma integrada y organizada permiten prestar el servicio oportunamente a los usuarios finales de las entidades a las que se le ofrecen los productos y servicios.

Se hace cada vez más imperativo determinar los riesgos, amenazas y requisitos de disponibilidad sobre los cuales se debe potenciar los procesos de SISTESEG para responder a los retos que se plantea día a día.

El principal beneficio de la planificación de la continuidad del negocio, es ayudar a identificar más claramente los riesgos potenciales a los que pueda ser vulnerable, reconociendo además lo que necesita para asegurarse contra.

Con base en las mejores prácticas definidas por el DRII[2], BCI e ISO 22301:2012 e ISO 27031:2011 en términos de proyectos de DRP, esta propuesta incluye las fases de Análisis de Impacto de Negocio, Evaluación de Riesgos Operacionales y Análisis de Estrategias de Recuperación ante desastres según los escenarios de riesgo y una parte de capacitación.

[2] Disaster Recovery Institute International

La norma ISO 27031:2011 comprende todos los eventos e incidentes que se relacionan con la seguridad de la información y pudiesen tener un impacto en la infraestructura y los sistemas TIC. La norma tiene como objetivo proporcionar la continuidad de los servicios prestados por el departamento de TI para los otros procesos de la organización.

1.2 SOLUCIÓN PROPUESTA

El objetivo del DRP es sostener en niveles previamente definidos y aceptados, los productos y servicios críticos a través de la estructuración de procedimientos e información en lo relacionado a productos y servicios, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre.

Teniendo en cuenta los requerimientos planteados por SISTESEG en torno a la necesidad de establecer un DRP que contempla las siguientes cuatro fases principales:

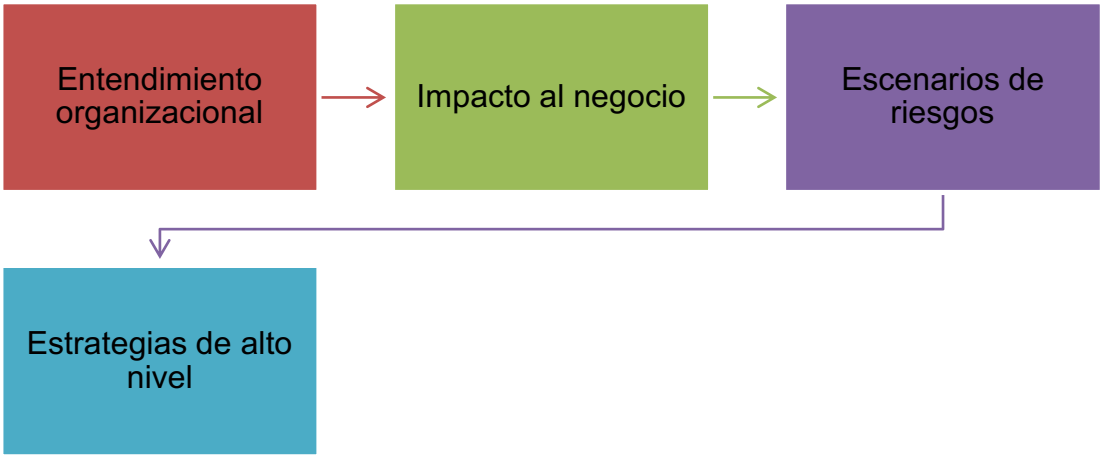


Figura No. 1. Etapas del DRP, ISO 27031:2011.

Planes adicionales al BCP

Entre los planes adicionales al BCP, la siguiente figura, basada en la publicación especial del National Institute of Standards and Technology, NIST, SP800-34, se observa una versión holística de los diferentes tipos de planes relacionados con la atención de desastres, incidentes y emergencias, que se interrelacionan con la GCN, la complementan y la apoyan:

Figura No.4. Planes complementarios al BCP.

Del análisis inicial de la figura anterior, se puede observar la eventual conveniencia de que la Gestión de la Continuidad del Negocio (GCN), se complemente con una serie de planes adicionales con funciones específicas. Sin embargo, debido a la carencia de definiciones estandarizadas para estos tipos de planes, en algunos casos, el alcance y su implementación puede variar entre las diferentes organizaciones. Por ello, se considera conveniente, como se hará a continuación, contar con una definición precisa de cada uno de estos planes complementarios e importantes a la GCN.

- **Plan de comunicación de crisis**: este documento debe describir los procedimientos y comunicados de prensa que las organizaciones deben preparar para responder ante un incidente de manera correcta. Este plan debe estar coordinado con los otros planes de la organización para asegurar que sólo comunicados revisados y aprobados sean divulgados y que solamente el personal autorizado, previamente designado, sea el responsable de responder las diferentes inquietudes y de diseminar los reportes de estado a los empleados y al público en general.

- **Planes de evacuación por edificio**: estos planes, contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.

- **Plan de respuesta a ciberincidentes**: este plan establece los procedimientos para responder a los ataques en el ciberespacio contra los sistemas de información de una organización. Estos planes son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como:

acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados a hardware, software, entre otros. Ejemplos de elementos que pueden generar incidentes de seguridad se tienen: la lógica maliciosa, los virus, los gusanos, los Troyanos. Estos planes normalmente pueden pertenecer o estar integrados al Sistema de Gestión de la Seguridad de la Información (SGSI).

- **Plan de recuperación de desastres (PRD)**: este plan es conocido como DRP (Disaster Recovery Plan), por sus siglas en inglés, está orientado a responder a eventos importantes, usualmente catastróficos, que puedan afectar la prestación de los servicios de información. Frecuentemente, el DRP se refiere a un plan enfocado en TI, diseñado para restaurar la operatividad de los sistemas, aplicaciones y bases de datos, además, se cuenta generalmente con un sitio alterno en donde se realizarían las operaciones que fueron interrumpidas por el incidente en el sitio principal. El alcance de un DRP puede confundirse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieren reubicación. Este es el plan que es objeto de esta propuesta.

- **Planes de contingencia**: Según el NIST, los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y a recuperar los servicios críticos de TI después de una emergencia en un tiempo mínimo. Es posible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contigencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective: Tiempo Objetivo de Recuperación), muy cercano a cero. Los planes de contigencia son típicos en los canales de comunicaciones, de tal manera que ante la falla de uno de estos canales, otro, entrará en operación muy rápidamente y en muchos casos de manera automatizada.

1.3 CONTEXTO ORGANIZATIVO

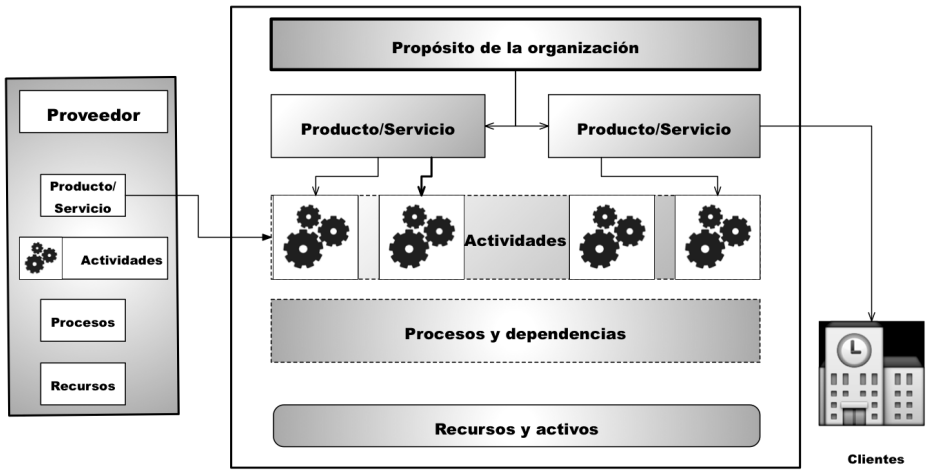


Figura No. 2. Entendiendo la organización.

Etapa 1. Análisis de Impacto de 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 BCP. 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 y productos críticos con el fin de regresarlos a su operación normal después que ha ocurrido un desastre y los tiempos de almacenamiento requeridos para disminuir el impacto.

El BIA implica también determinar las labores y los recursos esenciales para respaldar la continuidad de las operaciones, su criticidad, su impacto para el negocio, sus RTO´s (Recovery Time Objective – tiempo de recuperación objetivo) y RPO´s (Recovery Point Objective - punto de recuperación objetivo)[3].

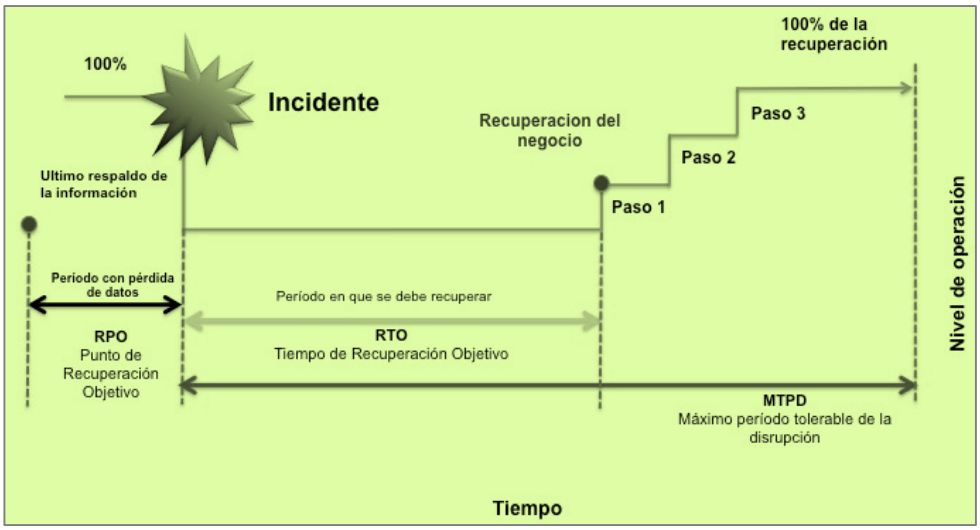


Figura No. 6 Tiempos de recuperación.

- Identificar los MTPD[4] de los productos y servicios críticos del negocio (ISO 22301)
- Mapear servicios/procesos de negocio vs aplicativos para identificar relaciones entre procesos y tecnología (ISO 22301)
- Definir tiempos de recuperación a partir de la criticidad de los proceso de negocio: RPO y RTO
- Definir los servicios mínimos que se deben habilitar en contingencia

[3] 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.

[4] Tiempo máximo tolerable de disrupción.

- Definir las aplicaciones críticas de negocio

Etapa 2. Evaluación de Escenarios de Riesgos Operacionales en TI:

- Identificar los escenarios de riesgos
- Identificación de amenazas que pueden afectar la continuidad operacional
- Determinación de niveles de impactos y probabilidades de ocurrencia
- Elaboración del mapa de riesgo de continuidad operacional en TI

Etapa 3. Análisis de las estrategias en TI:

- Diseño de escenarios de estrategias de continuidad operacional – teniendo en cuenta requerimientos de Análisis de Impacto de Negocio, Evaluación de Riesgos y premisas definidas por el negocio
- Evaluación de las diferentes estrategias de continuidad operacional a través de la relación costo estimado de manera cualitativa y el beneficio
- Realización de la matriz de estrategias
- Esta fase no comprende el diseño detallado o general de alguna de estas estrategias, y las estrategias son solamente para el área de tecnología

1.4 ALCANCE DETALLADO DEL PROYECTO

Con el fin de establecer una estrategia más detallada del plan de continuidad entorno a la operación de sus recursos, nos permitimos plantear como alcance del proyecto las fases de:

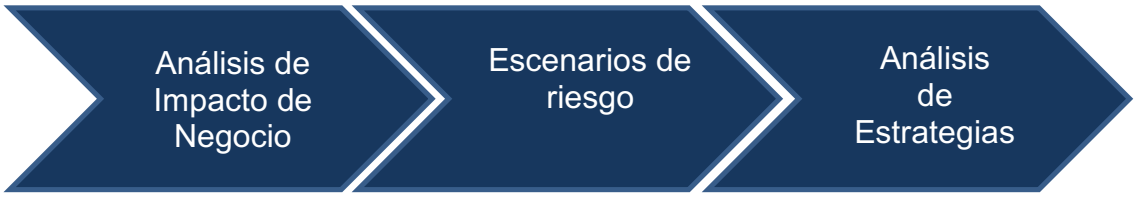


Ilustración 2. Fases del proyecto.

A continuación se muestran las actividades principales que comprende un BCP, desde la identificación de los servicios y productos críticos de la organización hasta definir las diferentes estrategias de recuperación dependiendo de los escenarios de riesgos:

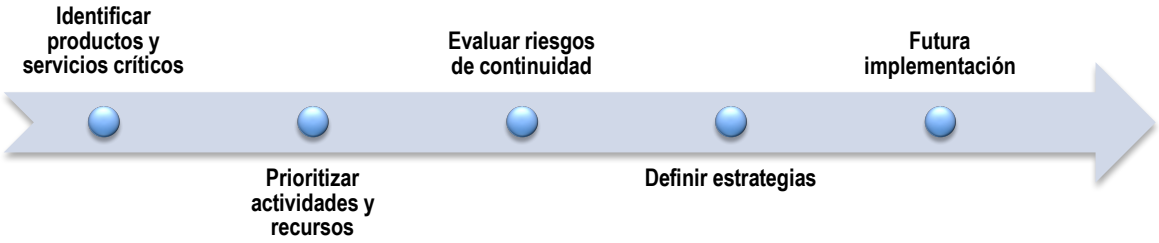


Ilustración 3. Actividades iniciales.

1.5 ANÁLISIS DE IMPACTO DE NEGOCIO (BIA).

La etapa de Análisis de Impacto de Negocio tiene como objetivo principal proporcionar a los requerimientos de información necesarios para el diseño de la estrategia de Continuidad Operacional de sus recursos que soportan a los procesos y productos de las AREAS DE NEGOCIO.

A través de la identificación, calificación y cuantificación de los impactos generados por una interrupción de las operaciones, son definidas los procesos de negocio y los sistemas de información/componentes y recursos que requieren el más alto nivel de disponibilidad y protección.

De esta forma, durante esta etapa serán definidos y priorizados los tiempos de recuperación (MTPD, RPO y RTO) por procesos de negocio y/o servicio, los recursos mínimos requeridos en contingencia como número de sedes/unidades y número de usuarios finales, y la secuencia de recuperación de acuerdo a la criticidad identificada.

El resultado de este análisis es muy relevante ya que sustenta ante la Alta Dirección la necesidad de implementar una o varias estrategias de continuidad operacional, mediante la identificación de los impactos que pueda generar una posible interrupción de la prestación de los productos y servicios críticos de la organización.

Al finalizar esta etapa se contará con los elementos necesarios para diseñar la estrategia de continuidad operacional de los Sistemas durante la etapa de “Diseño de la estrategia”, también incluida en el alcance de esta propuesta.

Tipos de BIA	Definición
BIA estratégico	Identifica y prioriza los productos y servicios más urgentes y determina los tiempos de recuperación y el impacto a la disrupción desde un punto de vista estratégico.
BIA táctico	Se determinan los procesos requeridos para la entrega de los productos y servicios críticos y se analizan los impactos por interrupciones.
BIA operacional	Se identifican y se priorizan las actividades en los procesos determinados como críticos y se determinan los recursos requeridos.

Tabla No. 1. Tipos de BIA ofrecidos como valor agregado dentro del proyecto.

Alcance

Metodología

Las actividades que se contemplan desarrollar con las AREAS DE NEGOCIO BCP durante la etapa de Análisis de Impacto de Negocio serán las siguientes:

- Mapeo de procesos de negocio y los productos y servicios críticos
- Evaluación cualitativa de los impactos financieros, operativos y de pérdida de imagen generados por una interrupción de las operaciones.
- Definición de los tiempos de interrupción (MTPD, RTO y RPO) a partir de la criticidad de los procesos de negocio y/o servicios.
- Recursos requeridos por procesos misionales

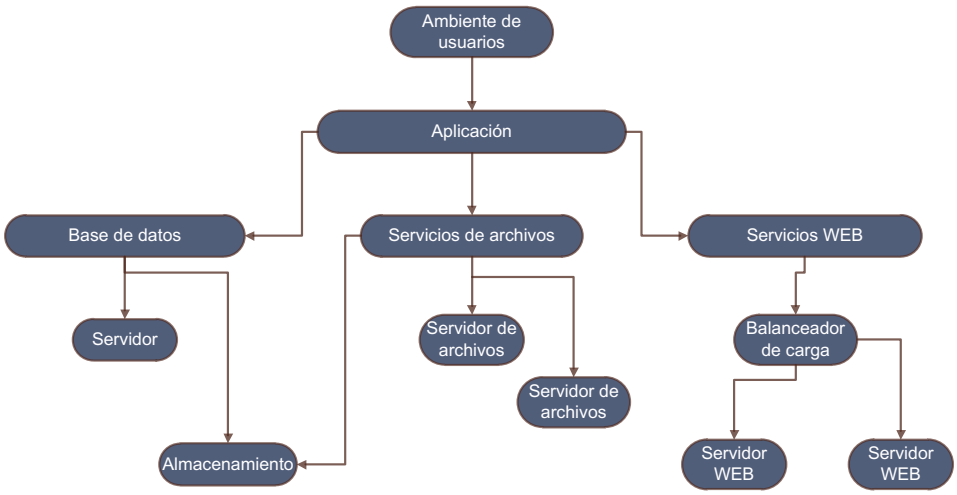


Ilustración 4. Diagramas de dependencia.

Las anteriores actividades serán desarrolladas a través de sesiones de entrevistas, encuesta y talleres para la recolección de datos del BIA, y sesiones de validación y priorización de resultados para la identificación de requerimientos finales. Por esta razón el alto compromiso que se requiere por parte de los líderes y gerencias de negocios.

1.6 ESCENARIOS DE RIESGO Y SU ANÁLISIS (RA)

La etapa de escenarios de riesgo en TI tiene como objetivo principal identificar las amenazas y los riesgos a los que está expuesto a SISTESEG respecto a la continuidad de las operaciones y generar así los escenarios de riesgo del negocio.

Del mismo modo que en la etapa anterior, el análisis de escenarios de riesgos permite sustentar ante la Alta Dirección la necesidad de implementar una estrategia de continuidad operacional, mediante la identificación de las amenazas y vulnerabilidades que puedan ocasionar una interrupción parcial o totalmente las operaciones.

Como resultado de esta etapa, SISTESEG recibirá un mapa de riesgos donde se identificarán los diferentes escenarios de riesgos que puedan afectar la continuidad operacional de la organización, incluyendo sus probabilidades de ocurrencia y los impactos que puedan generar sobre la organización.

Así mismo, esta etapa proporcionará los requerimientos necesarios para diseñar la estrategia de continuidad operacional de sus servicios y de sus sistemas de información durante la etapa de “Diseño de la estrategia”, también incluida en el alcance de esta propuesta.

NOTA: La evaluación de riesgos operacionales NO incluye los siguientes aspectos:

- Verificación de la efectividad de controles
- Cualquier otro punto que no sea incluido en el alcance de la actividad Evaluación de Riesgos Operacionales

Metodología

Las actividades contempladas ejecutar son:

- Identificación de escenarios de riesgos en TI
- Identificación de amenazas que puedan afectar la continuidad operacional en TI
- Determinación de niveles de impactos y probabilidades de ocurrencia
- Elaboración de un mapa de riesgo con el resumen de los riesgos identificados (ver figura abajo)
- Identificación de controles actuales y recomendados

Las anteriores actividades serán desarrolladas a través de sesiones de entendimiento de la plataforma tecnológica que soporta los procesos misionales; entrevistas, encuesta y talleres para la recolección de información de activos, amenazas y controles, y sesiones de validación y priorización de resultados para la identificación de los requerimientos finales. Por esta razón el alto compromiso que se requiere por parte de los líderes de la organización.

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

Ilustración 5. Mapas de riesgo.

1.7 ANÁLISIS DE LAS ESTRATEGIAS DE CONTINUIDAD OPERACIONAL

La etapa de Estrategias de Continuidad Operacional tiene como objetivo principal analizar los diferentes esquemas de continuidad operacional para los sistemas de tal forma que cumplan con los requerimientos reflejados por el Análisis de Impacto de Negocio y la Evaluación de Riesgos Operacionales.

Los esquemas de continuidad operacional contemplan los componentes a **alto nivel** de hardware, software, comunicaciones, centros de cómputo, servicios de operaciones y demás elementos necesarios para implementar una estrategia completa de continuidad operacional y que esté alineada con los requerimientos del negocio.

Teniendo en cuenta que existen diferentes soluciones en el mercado para cumplir con estos requerimientos se presentarán diferentes alternativas a nivel de mecanismos de replicación, hardware, software, centros de cómputo, personas, información, instalaciones y esquemas de prestación de servicios, etc. con el objetivo de poder encontrar una relación costo-beneficio entre los diferentes esquemas.

El resultado de esta fase de diseño es muy relevante para SISTESEG, ya que entrega un resumen de cuáles son las estrategias de continuidad operacional que se recomiendan se deberían implementar, cuáles son sus costos asociados y por ende cuál es el presupuesto que se debería destinar para estos proyectos que se desprenden de cada estrategia y que no son parte del alcance de esta propuesta.

Metodología

Las actividades que se desarrollarán durante la etapa de Análisis de Estrategias de Continuidad Operacional serán las siguientes:

- Análisis de alternativas de estrategias de continuidad operacional (ver tabla abajo)
- Evaluación de las diferentes alternativas de estrategias de continuidad operacional a través de la relación costo beneficio
- Requerimientos generales a nivel de tecnología, personas, instalaciones e información

Las anteriores actividades serán desarrolladas a través de sesiones de trabajo con el equipo de la empresa con el objetivo de definir las premisas generales de las estrategias de continuidad operacional. Respecto al diseño de las estrategias de continuidad operacional y la elaboración de la relación costo beneficio serán desarrollados por el grupo de especialistas y arquitectos.

Sitio	Costo	Hardware	Telecomunicaciones	Tiempo	Localización
Sitio en frío	Bajo	No	Ninguno	Largo	Fijo
Sitio preparado (hot site)	Medio	Completo	Completo	Corto	Fijo
Sede admin alterna	Alto	Variable	Variable	Variable	No fijo
Espejo (Mirror)	Muy Alto	Completo	Completo	Ninguno	Fijo
Personal externo	Medio	Por demanda	Completo	Corto	Fijo

Estrategias generales de recuperación

2 DEFINICIONES DE LA GCN

SANS[5]: La continuidad del negocio se refiere a las actividades requeridas para mantener su organización operando durante un periodo de desplazamiento o interrupción de la operación normal.[6]

BCI[7]: La continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre.

DRI international[8]: La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

NIST[9]: El BCM se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recupera paralelamente. El BCM se orienta hacia los productos y servicios críticos. Por su parte, el DRP provee procedimientos detallados para facilitar la recuperación de las capacidades en sitio alterno. Normalmente está enfocado en Tecnologías de la Información (en adelante TI) y limitado a interrupciones mayores con efectos a largo plazo. Los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI después de una emergencia. Debido a que los planes de contingencia deben ser desarrollados para cada aplicación importante o sistema de soporte, se pueden contar con múltiples planes de contingencia dentro de un BCP.

BRITISH STANDARS (BSI) & BS 25999: La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCM al día.

[5] SysAdmin, Audit, Network, Security, para mayor información consultar: http://www.sans.org
[6] Traducción del autor del documento.
[7] Business Continuity Institute, http://www.thebci.org/
[8] Disaster Recovery Institute Internacional: https://www.drii.org
[9] National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34.

3 BIBLIOGRAFÍA

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2012) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2012) – Societal security – Terminology

ANEXO: Control de Cambios

A continuación, el formato que se diligencia como parte del proceso de control de cambios y que documenta estas situaciones.

	FORMATO DE CONTROL DE CAMBIO		Contrato N.°: Cambio N.°:
CLIENTE:			
PROYECTO:			
INFORMACIÓN			
Solicitado por:		Fecha:	
Descripción del cambio:			
APROBACIÓN PARA EL ANÁLISIS			
Por xxx: Sí / No:		Por (Cliente): Sí / No:	
Nombre y cargo:		Nombre y cargo:	
Fecha:		Fecha:	
ANÁLISIS			
Impacto general del cambio:			
Impacto en tiempo:	+/-	Impacto en RR. HH.	+/-
Impacto en precio:	+/- $	Con cargo a:	
Comentarios:			
Analizó en:		Analizó en (Cliente):	
Cargo:		Cargo:	
Fecha:		Fecha:	
APROBACIÓN			
Por xxx: Sí / No:		Por (Cliente): Sí / No:	
Nombre y cargo:		Nombre y cargo:	
Fecha:		Fecha:	
Observaciones:			