PLAN DE CONTINUIDAD DEL NEGOCIO

FIRMAS		
ELABORADO POR:	REVISADO POR:	APROBADO POR:
	Milagros del Pilar Ramos Aquino Jefatura Administrativa Servicios Digitales S.A.C.	Ing. María Ursula Buleje De la Roca GERENTE GENERAL SERVICIOS DIGITALES S.A.C.
SOPORTE TECNICO TI	ADMINISTRACION	GERENCIA GENERAL

FIRMAS Y REVISIONES

TITULO	PLAN DE CONTINUIDAD DEL NEGOCIO SERVICIOS DIGITALES SAC
AUTOR	Área de Soporte Técnico y Seguridad de la Información
TEMA	Seguridad y Privacidad de la Información
FECHA DE ELABORACIÓN	08 de Febrero 2019
FORMATO	PDF
VERSIÓN	0.1
PALABRAS RELACIONADAS	Sistema de Gestión de Seguridad de la Información – SGSI, Modelo de Seguridad y Privacidad de la Información – MSPI, Plan Estratégico de Tecnologías de Información y Comunicación – PETI, Plan de Seguridad Y Privacidad de la Información, Políticas, Confidencialidad, Integridad, Disponibilidad y Privacidad, Análisis de Impacto al Negocio.

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

El incremento de las amenazas externas e internas ha llevado a las entidades públicas y privadas a considerar la importancia de la implementación de planes, procedimientos, y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante eventualidades de diversas categorías y diferentes niveles de impacto. Estos factores, han llevado a que en la actualidad la presencia de estos planes sea un factor común a lo largo de la cadena de suministro de los productos y servicios.

Anteriormente las amenazas estaban ciertamente asociadas principalmente a contingencias de carácter natural y tecnológico, las amenazas cada vez se tornan en diferentes escenarios como es el terrorismo, paros a nivel nacional, la globalización y las ciber-amenazas que han mostrado la necesidad de incorporar nuevas estrategias con el fin de garantizar la continuidad de las operaciones ante un evento cada vez más dinámico en la relacionado con el tipo de riesgos al que se está expuesto.

2. OBJETIVO

Establecer premisas y lineamientos a seguir ante un evento de interrupción, con el fin de continuar con las actividades críticas de la empresa SERVICIOS DIGITALES SAC.

3. ALCANCE

Inicia con la detección del evento de interrupción y finaliza con la estrategia de recuperación.

4. MARCO LEGAL

NORMA	DESCRIPCIÓN
NTC/ISO 22301:2012	Norma internacional para la gestión de la continuidad de negocio
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea.

5. DESARROLLO

5.1. GENERALIDADES

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.

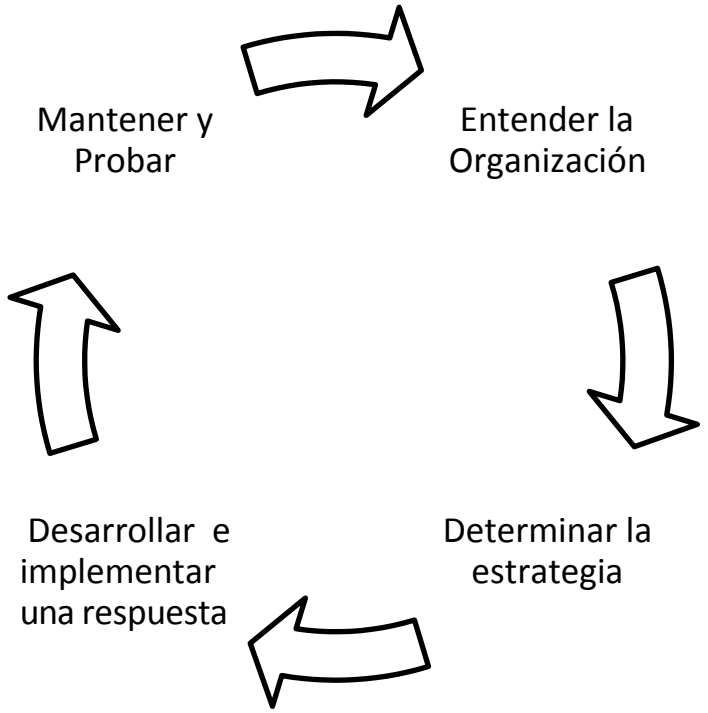
La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

La empresa SERVICIOS DIGITALES SAC, se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recupera paralelamente. La empresa SERVICIOS DIGITALES SAC, se orienta hacia los procesos de negocio. Por su parte, SERVICIOS DIGITALES SAC, 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 las políticas de la empresa SERVICIOS DIGITALES SAC.

Norma NTC/ISO 22301

La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales y riesgos de tipo operacional 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 las labores de la empresa al día.

En la siguiente ilustración se puede observar el ciclo de vida del programa BCM, que inicia en la fase de entendimiento de la organización, luego se definen opciones, se procede a la implementación, se realizan pruebas del plan o planes, su mantenimiento y auditorías tanto internas como externas, y, por último, se debe integrar este ciclo dentro de la cultura organizacional.



Ilustración

5.2. PLAN DE CONTINUIDAD DEL NEGOCIO

Se entenderá en este documento que el Plan de Continuidad del negocio de la empresa (SERVICIOS DIGITALES S.A.C.) busca sostener en niveles previamente definidos y aceptados, los procesos críticos del negocio 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. Por otra parte, el área de TI, tiene que tener predefinidos los planes de contingencia, que forman parte del plan de continuidad y están enfocados frecuentemente a recuperar los activos asociados a las Tecnologías de la Información. Por otro lado, el Plan de Continuidad del Negocio busca respaldar integralmente los intereses de las diferentes partes que intervienen en la organización, así como preservar los indicadores de generación de valor (reputación, marca, confianza, entre otros). Asimismo, se busca optimizar la capacidad de recuperación ante pérdidas significativas en recursos productivos u operativos (personal). Para el desarrollo del documento se utilizarán como referencia los estándares y las mejores prácticas DRII (Disaster Recovery Institute Internacional) e ISO 22301, entre otros. En total se consideraron 4 FASES como se puede ver a continuación:

Ilustración 2 Etapas

5.2.1. PLANES COMPLEMENTARIOS DE CONTINUIDAD DEL NEGOCIO

El plan de continuidad del negocio se relaciona directamente con otros planes los cuales complementan y apoyan la respuesta general de continuidad según sea el tipo de evento o el escenario correspondiente.

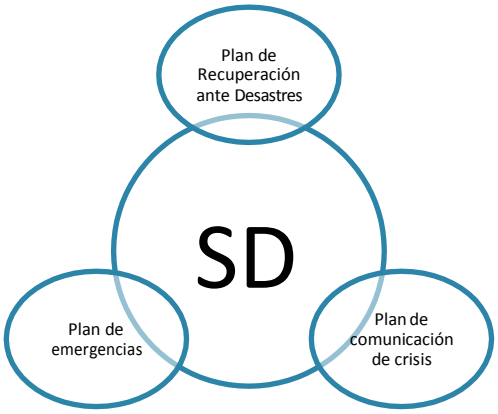


Ilustración 3 Planes

- **Plan de comunicación de crisis**

Documento que contiene los procedimientos internos y externos que las organizaciones deben preparar ante un desastre. Este plan debe estar coordinado con los demás planes para asegurar que sólo comunicados aprobados sean divulgados y que solamente el personal

autorizado 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 Emergencia**

Contiene 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 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 recuperación de desastres (DRP)**

Orientado a responder a eventos importantes, usualmente catastróficos que niegan el acceso a la facilidad normal por un período extendido. Frecuentemente, el DRP se refiere a un plan enfocado en TI diseñado para restaurar la operatividad del sistema, aplicación o facilidad de cómputo objetivo en un sitio alterno después de una emergencia. El alcance de un DRP puede solaparse 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. Dependiendo de las necesidades de la organización, varios DRP´s pueden existir.

5.3. METODOLOGÍA

La metodología utilizada para el desarrollo del Plan de Continuidad del Negocio para la empresa SERVICIOS DIGITALES SAC, propone un proceso comprendido desde el inicio del proyecto hasta el mantenimiento del plan. Esta metodología, está apoyada en mejores prácticas a nivel internacional proveniente de reconocidos institutos tales como el DRII, NIST, ISO 27001, NFPA 1600, entre otros.

1. Inicio del proyecto
2. Entendimiento de la organización
3. Análisis de impacto al negocio (BIA, Business Impact Analysis, por sus siglas del inglés)
4. Evaluación de riesgos
5. Estrategias de continuidad
6. Comité de crisis
7. Comunicaciones
8. Entrenamiento
9. Pruebas

5.3.1. INICIO DEL PROYECTO

Esta fase se realiza con el propósito de estructurar el proyecto para la empresa SERVICIOS DIGITALES SAC, de forma tal que éste se encuentre adecuadamente organizado y controlado durante su ejecución para cumplir los objetivos estipulados. Es fundamental contar con el compromiso de la Alta Dirección, conformar los equipos de trabajo, definir el plan detallado de trabajo, determinar la participación de expertos en el negocio de los diferentes procesos y áreas, así como detallar el alcance del proyecto.

Para la empresa SERVICIOS DIGITALES SAC, se definió la siguiente política de Continuidad del negocio.

POLÍTICA DE CONTINUIDAD DEL NEGOCIO

La empresa SERVICIOS DIGITALES SAC, hace todo lo que esté a su alcance para que en un tiempo óptimo, ante eventos adversos que afecten sus operaciones, los clientes y partes interesadas continúen recibiendo los servicios que la empresa SERVICIOS DIGITALES SAC, determina como servicios críticos. La empresa SERVICIOS DIGITALES SAC, establece como premisa ante un incidente o catástrofe la preservación de la vida e integridad de sus colaboradores, contratistas y demás partes interesadas; y el restablecimiento de los servicios de manera priorizada de acuerdo con la criticidad para el negocio y los niveles de servicio comprometidos con los clientes tanto internos como externos.

LINEAMIENTOS GENERALES

a. El plan de continuidad de negocio de la empresa SERVICIOS DIGITALES SAC, está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.

b. Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad del Negocio.

c. En caso de presentarse un incidente significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos.

d. Las etapas del Plan de continuidad deben ser ejecutadas por cada una de las dependencias de la Entidad, con la guía y coordinación de parte del área de Soporte Técnico y Seguridad de la Información.

e. Los Jefes o encargados de cada dependencia deben designar un Líder de Plan de Continuidad del Negocio, quien es responsable de apoyar las actividades del Programa de Plan de Continuidad de Negocios para la dependencia que representa.

f. Las diferentes etapas que conforman la fase de Prevención deben ser ejecutadas con la siguiente frecuencia:

- El análisis de impacto del negocio debe actualizarse por lo menos una vez al año o cada vez que un Líder de Proceso lo requiera, teniendo en cuenta los cambios de la entidad y sus necesidades.
- Se debe realizar por lo menos una prueba anual a las estrategias de contingencia definidas.

g. Los procesos críticos deben ser recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad del Negocio.

h. Los procesos o servicios de la entidad que sean desarrollados por terceros contratados deben disponer de planes de continuidad, para lo cual el funcionario interventor del contrato debe solicitar este documento y remitirlo al área de Soporte Técnico y Seguridad de la Información, donde se analizará la cobertura del mismo. Adicionalmente, se debe verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas, donde la Oficina de Sistemas e Informática debe coordinar con la dependencia responsable del contrato la ejecución de pruebas adicho plan.

i. Los planes de contingencia deben mantenerse actualizados, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, proceso, tecnología; siendo necesario que en dicha revisión participen los líderes de los procesos involucrados.

5.3.2. ENTENDIMIENTO DE LA ORGANIZACIÓN

Durante esta fase se recopila la información de los procesos documentados de la empresa SERVICIOS DIGITALES SAC, y se revisan sus entradas, salidas y activos que requiere el proceso para lograr sus objetivos. También se realizarán entrevistas con cada uno de los encargados de los procesos seleccionados como críticos con el fin de lograr un mejor entendimiento de la organización y así tener las entradas suficientes para proceder a realizar el Análisis de Impacto al Negocio. Esta fase se concentra principalmente en entender la misión, visión, prioridades del negocio, realizar el Análisis de Impacto al Negocio o BIA, y realizar análisis de riesgos.

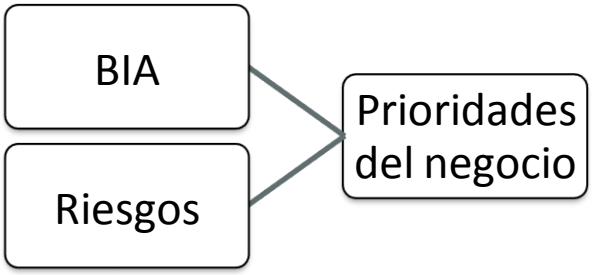


Ilustración 4. Entendimiento de la organización

5.3.3. ANÁLISIS DE IMPACTO AL NEGOCIO

El propósito del Análisis de Impacto al Negocio, conocido comúnmente como BIA, es determinar los productos y procesos críticos que garantizan la continuidad de las operaciones de la empresa SERVICIOS DIGITALES SAC, y los posibles impactos que se tendrían si éstos no se encuentran disponibles y en correcto funcionamiento. 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 la empresa SERVICIOS DIGITALES SAC, su criticidad, su impacto para el negocio, sus RTOs (Recovery Time Objective – tiempo de recuperación objetivo) y RPOs (Recovery Point Objective - punto de recuperación objetivo). También es parte del BIA el entendimiento y comportamiento de sus diferentes productos y servicios críticos.

Para el desarrollo del BIA, como se mencionó anteriormente, es muy importante, además de entender los productos y servicios críticos de la organización, analizar que procesos soportan la entrega de estos productos y servicios. Los procesos considerados fueron:

a. Procesos Misionales
- Docencia
- Investigación
- Capacitación
- Asesoría y Asistencia Técnica

b. Procesos de Apoyo
- Gestión Tecnológica
- Gestión Financiera
- Gestión Talento Humano

A continuación, se presentan las actividades, entradas y productos relacionados con la metodología del BIA:

1. Planeación del BIA
2. Levantamiento de la información
3. Análisis de la información
4. Informe de resultados
    - **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 la empresa SERVICIOS DIGITALES SAC, sobre los que se realizará el BIA.
2. Definir qué aspectos del negocio se desean cubrir con la información que se suministrará.
3. Identificar el personal a ser entrevistado.
4. Definir los cuestionarios a utilizar para recolectar la información, capacitar a los entrevistadores, unificar criterios y términos utilizados.
5. Definir las fechas en que se realizarán las entrevistas.

Levantamiento de información

En esta fase se realizan las entrevistas con el objetivo de recolectar la información necesaria para ser luego analizada en la siguiente fase (Análisis de la Información).

1. Realizar las entrevistas utilizando los cuestionarios diseñados en la fase de Planeación.
2. Inspeccionar físicamente los sitios.
3. Verificar a través de preguntas adicionales la veracidad de la información recibida.

Análisis de la información

En esta fase se procede a organizar, tabular y analizar la información recolectada, generando gráficas que permitan comprender de manera más sencilla los diferentes aspectos estudiados.

1. Analizar las cifras de impacto financiero y no financiero para cada uno de los procesos.
2. Analizar los hallazgos por proceso sobre los tiempos y puntos Objetivos de Recuperación (RTO, RPO) definidos por los entrevistados.
3. Consolidar la información de impactos financieros, no financieros, estacionalidad de los procesos y costos asociados a la reposición de los activos destruidos por un posible desastre.

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 procesos por el posible impacto financiero
2. Presentar la clasificación según el impacto no financiero
3. Presentar los activos que tendrán que ser adquiridos (reposición) como consecuencia de un posible desastre.
4. Generar observaciones sobre los resultados obtenidos.
5. Clasificar los procesos por su nivel de criticidad.

5.3.4. EVALUACIÓN DE RIESGOS

El propósito principal de esta fase es conocer cuáles amenazas o riesgos específicos enfrenta la empresa SERVICIOS DIGITALESA SAC, en sus procesos y productos 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.

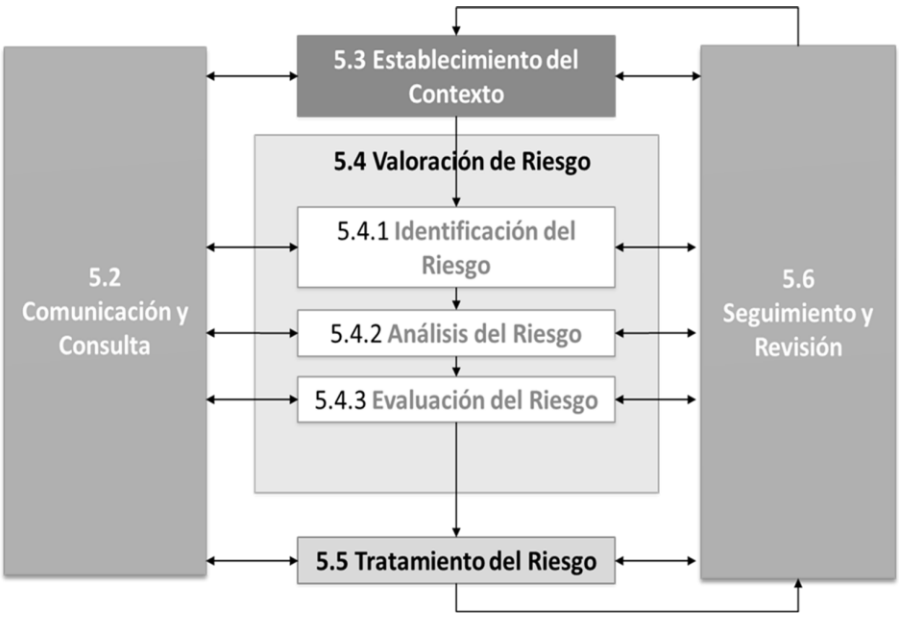


Ilustración 6. Análisis de Riesgos

Es conveniente mencionar que durante esta fase los riesgos (operativos) se analizarán desde la perspectiva de la continuidad del negocio considerando personas, servidores, edificios, tecnología, entre otros, 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. Ahora bien, parte importante de contar con un plan de continuidad, es el hecho de realizar una efectiva gestión de riesgo y así evitar las recursivas activaciones del sitio alterno, actividad que tiene sus propios riesgos, costos y dificultades.

En esta etapa, se analizaron las amenazas y vulnerabilidades identificadas previamente, analizando el escenario donde puede materializarse el riesgo de interrupción, así como su origen y las afectaciones potenciales a los activos, el análisis contempló 12 escenarios de riesgo que se describen a continuación:

1. **Acceso a la edificación:** Relaciona los controles, los procedimientos y las buenas prácticas que permiten mitigar el riesgo de que personal no autorizado ingrese a las instalaciones y pueda generar daños a los activos de la organización.
2. **Administración y entorno tecnológico:** Relaciona los hábitos y las buenas prácticas que permiten administrar, asegurar, disponer y controlar los sistemas tecnológicos, de tal forma que estén alineados con los estándares internacionales y regulaciones nacionales en temas de seguridad de la información.
3. **Construcción del edificio y materiales:** Relaciona los materiales de construcción, alternativas de mitigación y resistencia frente a riesgos naturales.
4. **Información y administración del edificio:** Relaciona procedimientos de seguridad, responsabilidades del personal, cultura y capacitación para responder a incidentes en el edificio.
5. **Oficina y estaciones de trabajo:** Relaciona las políticas de seguridad de la información definidas por la compañía y las buenas prácticas del personal que aseguren, en el evento de una interrupción del negocio, la disponibilidad, confidencialidad, seguridad e integridad de la información.
6. **Perímetro y estacionamiento:** Relaciona los controles, las políticas y los procedimientos que permitan evitar y responder frente a incidentes de seguridad en el perímetro de la compañía.
7. **Protección anti-incendios:** Relaciona la capacitación del personal, los equipos de extinción y los sistemas de control que permitan responder rápida y eficientemente a un incendio en el edificio y/o en el centro de cómputo.
8. **Riesgos entorno geográfico:** Relaciona las fuentes latentes de riesgo aledañas a la organización.
9. **Riesgos naturales:** Relaciona los aspectos de ubicación geográfica, climática y del entorno natural que puedan afectar a la compañía.
10. **Riesgos potencia eléctrica:** Relaciona las políticas, los controles y los procedimientos que permitan asegurar el suministro de energía eléctrica al edificio y equipos críticos.
11. **Riesgos telecomunicaciones:** Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.
12. **Centro de datos:** Relaciona, los controles, infraestructura y procedimientos definidos para

los centros de datos (principal y contingencia)

5.3.5. ESTRATEGIAS DE CONTINUIDAD

Una estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre 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 continuidades 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. Procesos críticos a soportar
4. Porcentaje aceptable de degradación de la operación del proceso.
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 asociados a los procesos.
7. Amenazas posibles a los activos de los procesos.
8. Vulnerabilidades existentes en los activos de los procesos.

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, 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.

Parte del desarrollo involucra la definición de los escenarios de interrupción, las amenazas que los pudieran generar y las diferentes alternativas operativas para enfrentar una posible materialización. En la siguiente tabla se visualiza la información referente:

	ESCENARIOS				
	Infraestructura No Disponible	**TI No Disponible**	**Recurso Humano No Disponible**	**Proveedor No Disponible**	**Información No disponible**
AMENAZAS	• Incendio, inundación, actos de violencia, terremoto • Cierre Parcial	• Falla Eléctrica • Incendio • Inundación • Terremoto • Falla tecnológica	• Incendio • Actos de violencia • Terremoto • Cierre Parcial • Ausencia, retiro, muerte de un funcionario	• Falla Eléctrica • Incendio • Inundación • Terremoto • Falla tecnológica	• Falla Eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas tecnológicasen: Comunicaciones, Hardware, Software, Bases de Datos • Error Humano • Hurto o Robo

	ESCENARIOS				
	Infraestructura No Disponible	**TI No Disponible**	**Recurso Humano No Disponible**	**Proveedor No Disponible**	**Información No disponible**
ALTERNATIVAS OPERATIVAS	• Trabajo a distancia • Acuerdo con Terceros • Respaldo entre sedes • Centro de Trabajo Alterno	• Estrategia DRP	• Definición de la Estructura de Recuperación en Cascada (ERC) • Capacitación • Rotación • Documentación de procedimientos	• Definir proveedores alternos • Definir Acuerdos de Niveles de Servicio específicos para BCM.	• Respaldo de la información clave del proceso (Backup) • Proveedores y/o medios Alternos para el servicio de comunicación

Tabla 1-Escenarios de Interrupción, amenazas y Alternativas Operativas

La siguiente es la relación de alternativas operacionales que tiene la organización, para recuperar la funcionalidad de sus procesos críticos en términos de la ausencia de alguno(s) de sus recursos claves, estas estrategias pueden permitir la continuidad de sus operaciones más importantes en un nivel aceptable y buscan principalmente cumplir y satisfacer los requerimientos del producto solicitado por sus clientes, después de un evento de interrupción:

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 NO DISPONIBILIDAD DE COLABORADORES DEL PROCESO	• Huelga de Colaboradores • Pandemia • Intoxicación Colectiva • Indisposición de Colaboradores (Ausencia, retiro o muerte)	• Definición de árboles de llamada. • Capacitación • Rotación • Documentación de procedimientos
 NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA	• Incendio • Inundación • Actos de Violencia • Sismo o Terremoto • Asonadas • Fugas de gas • Explosión	• Teletrabajo o home work • Acuerdo con terceros • Respaldo entre sedes (planta de producción) • Centro de Trabajo Alterno trabajo alterno para procesos administrativos

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 NO DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS	• Falla Eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos	• Estrategia DRP
 NO DISPONIBILIDAD DE INFORMACIÓN	• Falla Eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos • Error Humano • Hurto o Robo	• Respaldo de la información clave del proceso (Back Up) • Proveedores y/o medios Alternos para el servicio de comunicación
 NO DISPONIBILIDAD DE PROVEEDORES Y/O TERCEROS	No disponibilidad del Proveedor por eventos propios de su operación: • Falla Eléctrica • Incendio • Inundación • Huelgas o Asonadas • Pandemias • Actos de Violencia • Sismo o Terremoto • Fallas tecnológicas • No disponibilidad de sus Proveedores	• Definir proveedores alternos del servicio • Definir Acuerdos de Niveles de Servicio específicos para BCM

Tabla 2-Escenarios de Interrupción, Amenazas y Alternativas Operativas

5.3.6. COMITÉ DE CRISIS

El comité de crisis tiene como función principal la toma de decisiones en caso de que ocurra un desastre que cause la interrupción de los productos y servicios críticos de la empresa SERVICIOS DIGITALES SAC.

Entre las funciones principales podemos resaltar las siguientes.

- Analizar la situación para responder oportunamente.
- Tomar la decisión de activar o no el Plan de Continuidad
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.

- Definir un presupuesto estimado para gastos que genere la crisis.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.
- Tomar decisiones ante situaciones o imprevistos durante la recuperación de operaciones.
- Comunicar a los diferentes comités de la organización las decisiones que se tomen.

Para el caso de la empresa SERVICIOS DIGITALES SAC, se propone la creación de un comité de crisis conformado por los siguientes equipos:

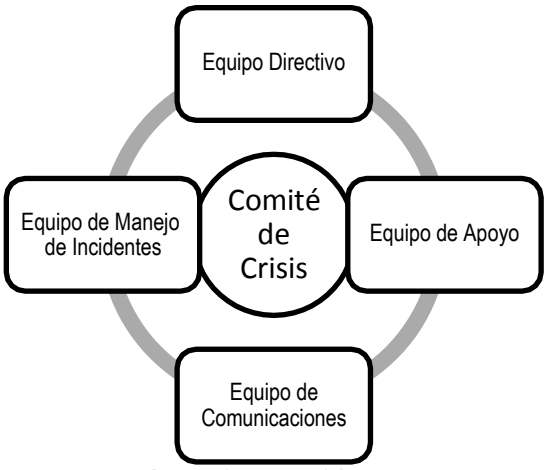


Ilustración 7. Comité de Crisis

- **Equipo Directivo**: Avala la decisión tomada por el Equipo de Manejo de Incidentes para la activación del Plan de Continuidad. Monitorea el incidente hasta su estabilización y retorno a la normalidad.
- **Equipo de Manejo de Incidentes:** Verifica el incidente, analiza las consecuencias e impactos potenciales, decide la activación o no del plan de continuidad y notifica al Equipo Directivo.
- **Equipos de apoyo:** Son los equipos necesarios para soportar la ejecución del Plan de Continuidad, cuando se les requiere.
- **Equipo de Comunicaciones:** Responsable del manejo de las comunicaciones con todas las partes interesadas.

5.3.7. COMUNICACIONES

Las comunicaciones tienen como función principal servir de apoyo para que en el caso de la ocurrencia de un desastre, se puede proceder de manera efectiva y eficiente a realizar el contacto de las diferentes personas que conforman el comité de crisis.

Ilustración 8. Estructura de comunicaciones

Por tanto, los equipos de comunicaciones son los equipos responsables de la elaboración y emisión de las comunicaciones corporativas hacia las partes interesadas tanto externas (entes de control, clientes, proveedores) como internas (Junta Directiva, colaboradores y sus familiares) durante y después de la crisis.

En la empresa SERVICIOS DIGITALES SAC, los responsables de las comunicaciones, operarán en contingencia de la siguiente manera:

- **Comunicaciones con los organismos de control:** El vocero oficial de la empresa SERVICIOS DIGITALES SAC, ante el comité primario.

- **Comunicaciones con las entidades externas y medios:** Área de comunicaciones

Los elementos utilizados por estos colaboradores para comunicarse con las entidades,

son:

- Correo electrónico
- Teléfono celular corporativo

La comunicación con los medios se realiza a través de correo electrónico y/o teléfono corporativo o de contacto

- **Comunicaciones con los colaboradores:** Líder de Gestión Talento Humano hacia los colaboradores y sus familias y líder de Gestión de la contratación para los contratistas.

Los elementos con los que cuenta este equipo para comunicarse internamente y para notificar la información correspondiente, son:

- Correo electrónico
- Teléfono celular corporativo
- Teléfono de la casa

6. DEFINICIONES

- **Análisis de impacto en el negocio:** Dentro de la gestión de la continuidad del negocio, es la tarea que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos de negocio, servicios TIC, etc.
- **Equipo funcional:** Colaboradores integrantes del proceso.
- **Evento de interrupción:** Un evento que impacta la capacidad de una organización para continuar sus operaciones.
- **Modalidad de Trabajo a Distancia:** Permite trabajar en un lugar diferente a la oficina. El trabajo se realiza en un lugar alejado de las oficinas centrales o de las instalaciones de producción, mediante la utilización de las nuevas tecnologías de la comunicación.
- **Plan de contingencia:** Un plan de respuesta de emergencia, las operaciones de backup y recuperación post-desastre gestionada por una organización como parte de su programa de seguridad que garantice la disponibilidad de recursos críticos y facilitar la continuidad de las operaciones en una situación de emergencia.
- **Plan de continuidad del negocio:** Recopilación documentada de los procedimientos y la información que se preparan para su uso en caso de incidente grave, con el objetivo de poder continuar prestando sus servicios críticos en un nivel aceptable pre-definido.
- **Políticas:** son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias.
- **Proveedor:** entidad encargada de abastecer un servicio o producto necesario para que desarrolle su actividad principal.