Lineamientos generales para el direccionamiento del Plan de Continuidad del Negocio – PCN en la empresa Savia Salud EPS

Por:

Natalia Vélez Muñoz

Tesis presentada para la obtención del título de:

Administradora de Empresas

Asesora Metodológica:

Isis Miosotis Álvarez

Universidad Autónoma Latinoamericana

Facultad de Administración de Empresas

Medellín

2019

Tabla de contenido

Listado de Tablas

Listado de Ilustraciones

INTRODUCCIÓN

Cuando las entidades hablan de *la continuidad del negocio,* se refieren a la capacidad institucional de **sobrevivir a las "cosas malas"** (Unipiloto, 2001)**,** que pueden impactar negativamente una empresa: un virus informático, incendios, desastres naturales o demás peligros que pueda ocurrir en la organización.

En consecuencia, la norma ISO 22301 de 2012, define la continuidad del negocio como, "la capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo" (ICONTEC, 2012). Por tanto, la organización debe planificar estratégica y tácticamente, como responder ante incidentes o interrupciones, de tal suerte que se garantice la supervivencia en el tiempo del negocio. La norma anterior expresa como se estructura un Plan de Continuidad de Negocio – PCN – este es aplicable al Sistema Integrado de Gestión de Savia Salud EPS.

En tal sentido, el plan consiste en una preparación proactiva de la organización frente a contingencias, mediante el desarrollo de mecanismos para restaurar los procesos clave, protegiendo el servicio al cliente y por ende la reputación de la compañía. Así mismo, el PCN se desarrolla para cubrir el peor escenario, de manera que escenarios menores queden cubiertos también.

Para la organización es importante que en el PCN se tracen unos objetivos, un alcance y toda una estructura orientada a las acciones para dar continuidad con las operaciones de la organización, para esto se identifican las actividades críticas, los recursos y personas que se necesitan para mitigar esos tiempos de interrupción y responsables de la ejecución del mismo; donde si se llega a materializar el riesgo, este plan pueda asegurar la recuperación de los servicios de Savia Salud EPS.

Finalmente, este documento ilustra el seguimiento y evaluación trazada en un tiempo determinado (anual) a los procesos misionales y el proceso de apoyo denominado Tecnología e Información –TI – como áreas críticas para Savia Salud EPS.

OBJETIVOS

1.1. Objetivo General

Establecer los lineamientos para el Plan de Continuidad del Negocio de SAVIA SALUD EPS que contenga las acciones requeridas para dar respuesta oportuna, frente a contingencias que comprometan la continuidad de la prestación del servicio.

1.2. Objetivos Específicos

- Identificar los procesos críticos, los recursos y los procedimientos necesarios para afrontar las eventualidades que puedan ocurrir en la organización.

- Mitigar los tiempos de interrupción de la operación de los procesos misionales y de Tecnología de Información, evitando la pérdida de información crítica para el negocio.

- Recomendar una estrategia de continuidad del negocio a partir de planes de recuperación de procesos.

2. ALCANCE

Aplica a sus procesos misionales y uno de apoyo TI, áreas críticas detectadas para la entidad cuya interrupción en el tiempo pueden afectar la operación de Savia Salud EPS.

3. JUSTIFICACIÓN

La continuidad del negocio es una de las principales iniciativas estratégicas que las organizaciones deben tener para asegurar su operación, esta entra en activación luego de presentarse eventos como desastres naturales (incendios, inundaciones, terremotos), ataque terrorista o daños en la infraestructura de TI que puedan cambiar las condiciones de la organización y así evitar que se generen inconvenientes económicos, pérdida de información y la no prestación del servicio.

Para ello, el PCN le permite conocer a Savia Salud EPS las condiciones tanto internas como externas que impactan los diferentes ámbitos del negocio, identificando las áreas críticas; compuesto el proceso misional por las siguientes tres procedimientos: Acceso, Aseguramiento y Autorizaciones y, el proceso de TI, conformado por cuatro procedimientos: Infraestructura y seguridad informática, Arquitectura, Software y Gestión de información y analítica de datos, y cómo debe ser el proceso para gestionar la seguridad infraestructura física y tecnológica, para la información siendo uno de los mayores activos de las organizaciones dado que dependen mucho de la tecnología, se debe tener en cuenta la implementación de un sistema alterno que resguarde toda la información de esas áreas críticas dentro del Plan de Recuperación de Desastres – DRP.

El PCN además de soportar el proceso de activación ante un desastre, sirve también como medio de identificación de riesgos, logrando así realizar acciones de control y evitar que se comprometa el desarrollo de las actividades cotidianas y futuras. El estar en el sector de aseguramiento, obliga a Savia Salud EPS a pensar en mecanismos de seguridad en cuanto a acciones clasificadas en los siguientes tipos de control: preventivos y correctivos; que deben realizarse para retomar en el menor tiempo posible la prestación de los servicios de salud a los afiliados. Este Plan da los lineamientos a seguir mediante estrategias que se articulen a otros planes que hoy tiene la organización, los roles responsables de la activación del plan y el seguimiento y la evaluación para la mejora permanente del PCN con el fin de proteger la entidad en un inicio con los procesos misionales y el de TI.

En este sentido, es importante la creación del PCN para Savia Salud EPS y de esta manera dar seguimiento y protección a los procesos que hacen parte del “Know How”, así como otros intereses en términos financieros, tecnológicos, infraestructura física, salud y seguridad de los trabajadores. Su construcción y metodología, están fundamentos en la norma ISO 22301 y en algunas normas específicas relacionadas con la gestión de riesgos de la Entidad Administradora de Planes de Beneficios en Salud – EAPB.

4. DEFINICIONES

Acción correctiva: Acción para eliminar la causa de una no conformidad u otra situación no deseada y prevenir su recurrencia.

Acción preventiva: Acción para reducir o eliminar un riesgo.

Activación: Acto de declarar que los acuerdos de la organización de Continuidad de Negocio deben llevarse a la práctica con el fin de continuar la entrega de productos o servicios clave.

Actividades priorizadas: Actividades a las cuales se les debe dar prioridad luego de la aparición de un incidente para poder mitigar los impactos.

Análisis de Impacto al Negocio: (BIA, por sus siglas en inglés, Business Impact Analisys) proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. Es un proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.

Auditoría: Proceso para obtener evidencia y evaluarla objetivamente para determinar el grado en que requerimientos específicos han sido alcanzados.

BCP: (Por sus siglas en inglés, Business Continuity Plan - Plan de Continuidad de Negocio), procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción

CDA: Comité de Desarrollo Administrativo

Continuidad de Negocio: Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

DRP: (Por sus siglas en inglés, Disaster Recovery Plan - Plan de Recuperación de Desastres), es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un

	incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.
Efectividad:	Grado en el cual actividades son realizadas y resultados planeados alcanzados.
Eficiencia:	Relación entre resultados alcanzados y los recursos usados.
Ejercicio:	Proceso para entrenar, evaluar, practicar, y mejorar el desempeño en una organización.
Evaluación del desempeño:	Proceso de determinar resultados medibles.
Evento:	Ocurrencia o cambio de un conjunto particular de circunstancias.
Incidente:	Situación que sería o podría llevar a una interrupción, pérdida, emergencia o crisis.
Infraestructura:	Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización.
Mejoramiento continuo:	Actividad periódica para mejorar el desempeño.
Monitoreado:	Observación de desempeño planeado.
Objetivo mínimo de continuidad de negocio:	(Minimum Business Continuity Objective por sus siglas en inglés) mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.
Parte interesada:	Parte afectada con interés en el éxito de una organización o actividad.
Plan de emergencias:	Documento que contempla las acciones e instrucciones que se deben seguir para responder rápida, eficaz y con el menor traumatismo posible ante una Emergencia.
Política:	Intenciones y dirección de una organización formalmente expresada por la alta gerencia.
Prueba:	Procedimiento para determinar la presencia, cualidad o veracidad de algo.
RPO:	(Por sus siglas en inglés, Recovery Point Objetive - Punto Objetivo de Recuperación), punto en el cual la información usada

por una actividad debe ser restaurada para permitir la reanudación de la operación.

Recurso: Todos los activos, recursos humanos, conocimientos, información, tecnología, locales y suministros e información que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

RTO: (Por sus siglas en inglés, Recovery Time Objetive -Tiempo objetivo de recuperación), periodo de tiempo después de un incidente en el que: El producto o servicio debe ser reanudado, o la actividad debe reanudarse, o los recursos deben ser recuperados.

Sitio Alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

Verificación: Confirmación, a través de la provisión de evidencias que especifican requerimientos que han sido alcanzados. (ICONTEC, 2012).

5. GENERALIDADES

El PCN tiende a operar en unas circunstancias que están sujetas a riesgos, cambios y oportunidades; dicha información ayuda a mejorar la formulación del plan con el fin de cubrir a largo plazo todo lo establecido dentro de él, siendo las partes interesadas, las necesidades y los requerimientos, elementos importantes a tener en cuenta, además de las siguientes consideraciones:

Seguir las indicaciones que la **Norma NTC/ISO 22301** sugiere para La Gestión de la Continuidad del Negocio (sus siglas en inglés - BCM), dado que este al ser un proceso de gestión integral, debe identificar las amenazas potenciales y los impactos que estas podrían causar a las operaciones del negocio; el contenido de la presente norma otorga los insumos para la construcción de la resiliencia empresarial con capacidad de dar una respuesta efectiva, que salvaguarde los intereses de las personas involucradas, la reputación de la entidad, su marca y las actividades que crean valor.

Savia Salud EPS cuenta con dos sedes en Medellín, las cuales, por sus condiciones de infraestructura física, cantidad de personas, accesos, servidores y demás cuentan cada una con un plan de evacuación; que deben ser utilizados en caso de presentarse una situación de emergencia. Este será igual para las demás sedes.

La comunidad donde la organización se encuentra ubicada, y que pueda ser impactada al momento de activarse el PCN según el tipo de riesgo, el proceso afectado, o si este es una emergencia institucional. Para ello debe de existir una articulación con los planes de las organizaciones cercanas y el de la función pública.

Conocer las necesidades de los grupos de interés hace parte de los factores a considerar para que el PCN se establezca y se implemente según las prioridades del negocio.

Mediante un periódico seguimiento y actualización de los elementos internos y externos de la organización, se logran alcanzar los resultados esperados en el PCN.

5.1. Análisis Situacional

En Colombia el sector de aseguramiento en salud "Es la principal estrategia del Sistema General de Seguridad Social en Salud (SGSSS) para lograr el acceso a la prestación de los servicios de salud incluidos en el Plan Obligatorio de Beneficios en Servicios de Salud POS, la Ley 1122 de 2007 define el aseguramiento como: la administración del riesgo financiero, la gestión del riesgo en salud, la articulación de los servicios que garantice el acceso efectivo, la garantía de la calidad en la prestación de los servicios de salud y la representación del afiliado ante el prestador y los demás actores sin perjuicio de la autonomía del usuario". (Departamento Nacional de Planeación - DNP, 2016).

Savia Salud EPS como entidad del sector salud, no está libre de la exposición a riesgos tanto externos como internos a los que es vulnerable una organización, por lo cual, debe gestionar de manera anticipada los eventos y/o vulnerabilidades por medio de la administración de riesgos en todos los procesos, a partir de un ciclo que consta de: identificar, evaluar, controlar y dar constante seguimiento a los riesgos que permiten mejorar la eficiencia operativa, la toma de decisiones y la mejora continua en los procesos.

Hoy la organización cuenta con un Sistema de Administración de Riesgos (SAR) y varios planes que se mencionan en el transcurso del texto, donde se propone el lineamiento a seguir en la gestión y monitoreo de los riesgos identificados, teniendo así las líneas frente al que hacer para cuando el riesgo se materialice y tener identificadas esas acciones de mejora para prevenir su materialización según el riesgo al que este expuesta la entidad; así mismo, a través de la Supervisión Basada en Riesgos (SBR), tiene documentado el Manual de Gestión de Riesgos MA-PN-02 y la Matriz de Riesgos FO-PN-05, encontrando así todos los riesgos de los procesos institucionales constituidos en dos tipos de inventarios, uno a nivel estratégico alineado a el cumplimiento de los objetivos estratégicos y otro a nivel operacional. Estos muestran todo el conducto a seguir del ciclo para la anticipación en la materialización de los riesgos, las acciones

para mitigar su impacto, los planes de mejora para disminuir su materialización y la totalidad de los riesgos institucionales identificados.

Los riesgos institucionales del SAR se gestionan basándose en las normas vigentes para el cumplimiento de requisitos mínimos exigidos por el Decreto 682 de 2018, las Resoluciones 4559 y 2515 de 2018 en cuanto a estándares y criterios de la gestión del riesgo, y la Circular Externa 004 del mismo año, referente a los requisitos mínimos que debe cumplir el SAR en la organización, para cada categoría de riesgo relacionada con su ciclo de identificación, evaluación y tratamiento.

En este marco, uno de los planes que tiene Savia Salud EPS, en pos de la respuesta a los riesgos a los que está expuesta la organización se evidencia en el documento “Plan de Prevención, Atención y Respuesta ante Emergencias” - OD-GH-03; este contiene todos los trazos en la identificación de riesgos externos, la metodología que dé cuenta del hacer en la probabilidad de ocurrencia y los análisis de vulnerabilidad.

Los anexos que documentan todos estos riesgos y procedimientos como el de “procedimientos operativos normalizados”, se encuentran construidos según el tipo de amenaza como pueden ser brote de enfermedades, infesta de animales, insectos o plagas, sismo o terremoto, licuación de suelos, deslizamientos, avalancha, inundaciones, vendavales, tormentas o rayos, vientos huracanados, incendios, explosión, fallas de estructura, fallas en los sistemas y procesos, obstáculos en las rutas de evacuación, entre otros. Estos procedimientos dan la línea de actuación mediante el flujograma, la descripción de cada acción que se debe realizar según el numeral y los responsables del mismo.

Con relación a este plan también es importante mencionar, que Savia Salud EPS tiene establecido el análisis de los riesgos externos según su naturaleza de carácter biológico, físico geológico, físico meteorológico, riesgo antrópico tecnológico, social, ambiental y, cada una de las amenazas pertenecientes a estos tipos de riesgos, tienen definidas las causas, sus análisis retrospectivos, la probabilidad de ocurrencia y el análisis de vulnerabilidad en las personas, recursos y sistemas.

Todo este cubrimiento de los riesgos externos se desarrolla de manera institucional, dado que cada proceso no tiene previsto escenarios externos más allá de lo que cubre el Plan. Se presenta así todo lo relacionado en cuanto a líderes de evacuación en las sedes, comité y brigada de emergencias, grupos de apoyo externos, registro de inventarios de elementos como extintores botiquín y demás elementos para atención de emergencia, así como lo que se tiene y que no de los inventarios en cada una de las sedes; sean estas en hospitales, centros comerciales y locales.

A su vez, el plan de contingencia habilita el proceso de las redes integrales de prestadores de servicios de salud, como EPS desde la Resolución 1441 del 2016; la cual permite la implementación de las Redes Integrales de Prestadores de Servicios de Salud – RIPSS como componente de la Política de Atención Integral en Salud – PAIS.) Conocido en la organización como "Plan de Contingencia para Garantizar la Continuidad en la Prestación de los Servicios de Salud" - OD-RS-08. Tiene desarrollado los riesgos para los cuales se activaría este plan, con su categoría, nivel de riesgo, causas, consecuencias y las acciones de contingencia en caso de materializarse.

También es importante mencionar que la dependencia de TI maneja todo el soporte técnico para la disponibilidad, habilitación y seguridad de la información, se tiene documentado en el "Manual de Política de Seguridad de la Información" – MA-TI-01, las medidas de índole técnico y administrativo, necesarios para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (voz y datos) que se utilizan en Savia Salud EPS; así mismo el procedimiento de soporte tecnológico mesa de ayuda, considerándose este como el primer nivel de dirección para realizar una solicitud frente a una emergencia del soporte técnico.

El esquema de contingencia con el que cuenta hoy la organización está documentado en el "Plan estratégico de tecnologías de la información y comunicación" – OD-TI-07; la infraestructura está soportada actualmente con el proveedor TIGO, contratado con dos Data Center certificados (centro de datos). Uno de ellos ubicado en Medellín, edificio inteligente; resguarda el 100% de la información en tiempo real, todo el aplicativo misional y el soporte operacional, el segundo se

encuentra ubicado en Bogotá, el cual tiene aproximadamente el 40% del soporte operacional. Según datos del componente de infraestructura del plan en mención, todo lo que tiene que ver con ofimática, data estadística, base de datos de producción (información), sin tener el aplicativo *Integra* (misional) en este centro. Esto se piensa cubrir de manera completa cuando entre a operar el proyecto de *Somos +*.

Por otra parte, la norma ISO 22301 articula el PCN con los planes estratégicos, de emergencias y contingencia; como también con el SAR, dado que la estructura de la norma proporciona una base de entendimiento, desarrollo e implementación para la continuidad de la operación dentro de la organización. Dicha norma también especifica los requisitos necesarios para planificar, establecer, operar, monitorear, revisar, mantener y mejorar de forma continua; con ello, se busca responder y poder recuperarse de las posibles interrupciones en la prestación del servicio.

Para comenzar con la formulación del plan se tiene en cuenta el mapa de procesos, teniendo un reconocimiento de los catorce (14) macroprocesos, que componen el funcionamiento dentro de la entidad, estos se encuentran segmentados según la gestión y operación a cargo; el PCN inicia incluyendo dos macroprocesos, uno misional conocido como *Realización* abarcando toda la prestación de servicios de salud y el segundo de apoyo ubicado en la *Gestión de Recursos.* Para mayor detalle es importante mencionar que en la formulación del PCN se deben identificar los procesos críticos del mapa (resaltados en círculos rojos), como se observan en la siguiente gráfica:

Mapa de procesos

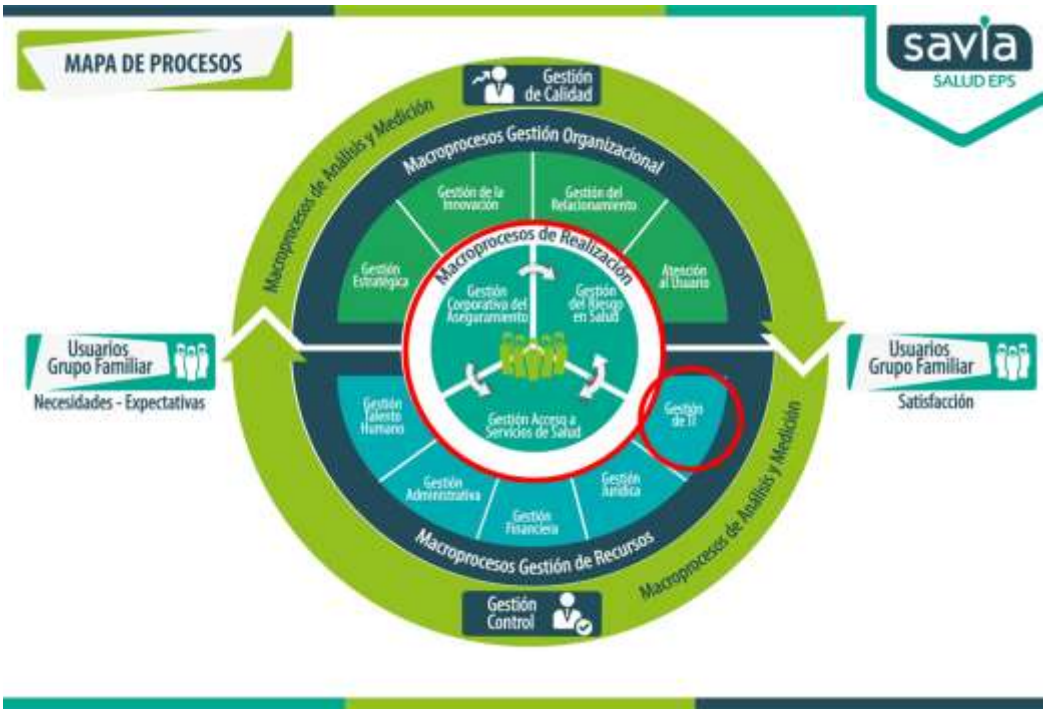


Ilustración 1 Mapa de proceso de Savia Salud EPS
Fuente: Elaborado por Gestión de Calidad

El PCN debe seguir incluyendo los 12 macroprocesos restantes de manera anual, según el alcance que a este se le quiere dar para tener un cubrimiento total y así llegar a un normal funcionamiento de todos los procesos de la entidad luego de presentarse un evento disruptivo; la medición es necesaria para detectar que proceso tiene mayor riesgo de perder información, procedimientos u otros recursos necesarios para que la organización siga en funcionamiento, al tener en cuenta que la medición del nivel de criticidad para cada uno de los procesos, es necesaria no solo en el momento de hacer la integración y generar ese respaldo que proteja lo misional, sino también los demás procesos de apoyo y de gestión estratégica, aproximándonos así a una posible recuperación total de Savia Salud EPS frente a un evento disruptivo.

6. LIDERAZGO

El desarrollo del PCN demuestra un compromiso desde la alta dirección conformada por un comité de emergencia encabeza del Gerente, Subgerentes, Directores, Jefes y los demás grupos de interés como son los socios, junta directiva, empleados, la comunidad y las organizaciones aledañas, desde la participación y cumplimiento con las responsabilidades que sean asignadas; con la capacidad para responder por cada una de las actividades que colocan en operación el plan, en caso de materializarse la interrupción de su funcionamiento.

6.1. Compromiso Alta dirección

La gestión que realiza la alta dirección es articular PCN con la dirección estratégica de la organización, esto trae consigo la integración del proceso misional y los de apoyo para el plan, con la capacidad de proveer los recursos necesarios para establecer, implementar y mantener la mejora continua de la gestión de continuidad del negocio; además está a cargo de comunicar la importancia del desarrollo y efectividad del plan, que aseguren los resultados esperados.

6.2. Política

Savia Salud EPS como Entidad Administradora de Planes de Beneficios en salud, gestiona el aseguramiento de la población pobre y vulnerable, para impactar en la calidad de vida de sus afiliados, por tal razón se compromete en la formulación de un Plan de Continuidad del Negocio con las medidas necesarias, que permitan direccionar los procesos misionales y el proceso de apoyo Gestión de TI que garantizan la continuación de la operación, de la siguiente manera:

1. Gestión del aseguramiento, el acceso y la gestión del riesgo de la salud para sus afiliados soportado en un sistema de información que facilite la identificación, valoración, control, evaluación y seguimiento en los niveles de riesgo.

2. Capacidad de asegurar la confidencialidad, integridad y disponibilidad de la información mediante la unidad de mando integral y todo lo relacionado con la gestión de seguridad de la información.

3. Para lograr lo anterior, la Alta Dirección mediante el Comité de Emergencias son los que asignan los recursos presupuestales, tecnológicos y las personas en los cargos necesarios, que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

6.3. Responsabilidades – Roles

Desde la Alta Dirección se delega la responsabilidad y autoridad de cada una de las acciones a desarrollar para la gestión del PCN en concordancia con lo sugerido por la norma ISO 22301 y las necesidades de Savia Salud EPS para continuar con su operación.

A continuación, se define la estructura del PCN donde se identifican las acciones y los responsables para la implementación, monitoreo, ejecución y la mejora continua del plan, con el objetivo de permitir la continuidad en la prestación de los servicios en salud para los afiliados.

6.3.1. Comité de Continuidad:

Conformado por la alta dirección de la empresa y gestiona administrativamente las decisiones en el momento de una crisis o emergencia. Es el equipo responsable de garantizar estratégicamente la coordinación de las actividades en cuanto al proceso de prevención, atención, mitigación y recuperación de la operación después de materializado el evento disruptivo.

Comité de Continuidad	
Responsables	**Responsabilidades Generales**
-El Gerente, o su delegado (director de continuidad)	Revisar y aprobar la política y las estrategias de continuidad del negocio, validando la asignación de

-Subgerente Desarrollo Organizacional, (coordinador de emergencias) -Subgerente Financiero -Subgerente de Salud -Director de Acceso Servicios de Salud -Director de Aseguramiento (coordinador de recuperación) -Secretaria General (apoyo jurídico) -Jefe de Comunicaciones (información y comunicaciones) -Jefe Gestión Administrativa (protección de bienes, mantenimiento y seguridad) -Jefe de Gestión Humana (líder evacuación) -Jefe Brigada de Emergencias	recursos para el momento de activación. Asegurar que el PCN sea compatible con la dirección estratégica de Savia Salud EPS (Ruta 19-28). Proveer suficientes recursos y/o proveedores externos, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el PCN. Desarrollar proyectos e iniciativas que posibiliten la preparación para atender una situación de contingencia, emergencia o desastre, facilitando la protección de las personas y la recuperación de la operación normal de la organización. Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados. Acordar con los responsables del PCN la estructura, dirección y conservar vigente la operación de los grupos de interés para la atención de situaciones de emergencia. Aprobar y/o rechazar las incorporaciones y/o modificaciones del PCN propuesta por los líderes y sus miembros. Definir y coordinar la aplicación de la metodología de identificación y medición del riesgo de interrupción del negocio en los procesos críticos. Involucrarse activamente en ejercicios y pruebas; cerciorando que las auditorías internas del PCN son conducidas a las revisiones de la dirección para lograr los resultados esperados. Administrar y utilizar la información perdida para monitorear la materialización del riesgo, y así reportar al Comité de riesgos aquellos eventos críticos de interrupción en la operación para la toma de decisiones.

-Jefe de Planeación y Gestión del conocimiento	Coordinar la ejecución de las actividades del plan según los ejercicios de pruebas.
-Jefe de Tecnología e Información (líder de Recuperación Tecnológica)	Responsable de la ejecución del PCN, cuando se presenten los eventos que lo activan.
	Socializar el PCN mediante los canales de comunicación que disponen Savia Salud EPS para todos los grupos de interés.
-Jefe de Autorizaciones (líder de Recuperación)	Verificar que el personal a su cargo se encuentre debidamente capacitado en la ejecución del PCN.
	Coordinar la capacitación al personal nuevo del servicio sobre las actividades que deben de ejecutar cuando se materialice el PCN.
	Participar en la definición de ajustes y planes de mejoramiento que se requieran a los procesos críticos.
	Reportar sus actividades directamente al Director General de la emergencia.
	Apoyar la operación contingente durante el incidente, siguiendo las estrategias planteadas en el PCN.
	Asumir el control y manejo de las comunicaciones dentro de la organización según la directriz del jefe de comunicaciones del Comité de Continuidad.
	Seguimiento anual del PCN de acuerdo a la política y estrategia del plan aprobada por la junta.
	Apoyo a la mejora continua, comunicando así la importancia de la efectividad del PCN.
	Toma de decisiones en cuanto a la activación según la crisis o emergencia que pueda materializarse.

Tabla 1 Responsables y responsabilidades generales del Comité de Continuidad
Fuente: Elaboración propia con datos de la norma y manual de comité de emergencias

Como se evidencia en la tabla 1, el Comité de Continuidad demuestra la importancia de su creación al contar con un equipo que pueda generar, coordinar y monitorear todas las acciones

necesarias, en el momento de tomarse la decisión de la activación del PCN y proteger la continuidad de la operación de la organización.

6.3.2. Comité de Emergencias:

Está conformado por la alta dirección de la organización y apoya en la ejecución del plan de continuidad, mediante la estructura en que se desarrolla el Plan de Emergencias, definiendo la ruta a seguir en los procedimientos antes, durante y después de una emergencia o desastre.

Comité de Emergencias	
Responsables	**Responsabilidades Generales**
-Director general del Plan de emergencias -Coordinador de emergencias (comandante del incidente) -Información y comunicaciones (oficial de información) -Protección de bienes, mantenimiento y seguridad -Coordinador de Evacuación -Jefe de Brigada de emergencias	Planear y organizar las diferentes acciones y recursos para la eficaz atención de una eventual emergencia.
	Conocer el funcionamiento de los procesos de la empresa y las organizaciones vecinas, las instalaciones, las emergencias que se puedan presentar y los planes normativos y operativos de las mismas.
	Identificar las zonas más vulnerables de la organización.
	Verificar la actualización del inventario de recursos humanos, materiales y físicos con los que puede contar los establecimientos de las sedes y los propios de la organización.
	Mantener el control permanente sobre las posibles situaciones de riesgo que se puedan presentar en la organización.
	Diseñar y promover programas de capacitación para todo el personal orientados a prevenir y afrontar emergencias.
	Evaluar los procesos de atención de las emergencias para realimentar las acciones de planificación.
	Definir políticas orientadas a la prevención de los riesgos de emergencias y desastres en la empresa.

	Asignar responsabilidades a la brigada de emergencias y líderes de evacuación de acuerdo a los planes de acción y recomendaciones del plan de prevención, preparación y respuesta ante emergencias.
	Activar la cadena de llamadas de los integrantes del comité de emergencias.
	Reunirse periódicamente y en el momento de una emergencia, para decidir las acciones a seguir frente a un evento, con el fin de mitigar, neutralizar y atender las situaciones de emergencia.
	Evaluar las condiciones y magnitud de la emergencia.
	Distribuir los diferentes recursos para la atención adecuada de la emergencia.
	Establecer contacto con los grupos de apoyo y con la ayuda externa (Policía, Cruz Roja, Defensa Civil, Bomberos, Tránsito, ARL), cuando se estime necesario.
	Tomar decisiones en cuanto a la evacuación total o parcial del establecimiento donde se presente la situación de emergencia.B40
	Reunirse en el sitio asignado como P.M.U (Puesto de Mando Unificado).
	Coordinar las acciones operativas en la atención de emergencias.
	Coordinar el traslado de los heridos a los centros de asistencia médica.
	Evaluar el desarrollo de las diferentes actividades contempladas en el Plan, después de cada emergencia o simulacro desarrollado.
	Presentar informes de dichas actividades a la Brigada de emergencias y demás organismos implicados en la cadena

	de respuesta según sea el caso.
	Permanecer en estado de alerta hasta “la vuelta a la normalidad” (recuperación).
	Retroalimentar cada uno de los elementos del plan de emergencias de la empresa.
	Establecer o determinar los correctivos pertinentes del plan.
	Verificar el cumplimiento de las actividades expuestas en el plan de acción de cada informe.

Tabla 2 Responsables y responsabilidades generales del Comité de emergencias
Fuente: Manual del Comité de Emergencias de Savia Salud EPS

En la tabla 2 se evidenciaron las acciones que el comité realiza de recuperación, retorno, planes de contingencia y normas de seguridad a tener en cuenta durante la ocurrencia del evento. Así el comité de emergencias activa el proceso de evacuación, y las prácticas de organizaciones vecinas a contemplar, forjando la importancia de consolidar un nivel de preparación frente a eventos que puedan representar pérdidas humanas o de la propiedad.

6.3.3. Planeación y Gestión del Conocimiento:

Esta dependencia marca todo un proceso esencial en cuanto a el acompañamiento en la creación de escenarios, identificación de riesgos, pautas metodológicas en el desarrollo de planes, así como definir los roles donde los empleados se comprometan con acciones responsables para proteger la información, y las personas mismas en algún momento de emergencia. Siendo así responsable de lo siguiente:

Proceso	**Planeación y Gestión del conocimiento**
Responsable	Jefe de Planeación

Misión del cargo	Dirigir las acciones según lo estipulado en el PCN que implique una respuesta según la estrategia creada para saber qué hacer en el momento de presentarse el evento, así mismo la activación del PCN en compañía del Comité de Continuidad hasta que hagan presencia las autoridades o los organismos de socorro externos, momento en el cual deben entregar este manejo a los respectivos responsables sin dejar de ser apoyo y fuente de información para una respuesta adecuada.
Funciones Específicas	Recopilar información necesaria para la construcción del PCN.
	Identifica, documenta y socializa las funciones y las responsabilidades de los roles del PCN.
	Reportar el desempeño del PCN a la alta gerencia.
	Definir el criterio para aceptar riesgos y niveles aceptables del riesgo según las necesidades mínimas de cada área critica para el PCN.
	Definir indicadores de eficiencia y eficacia, evaluarlos y tomar correctivos con base en los resultados obtenidos.
	Involucrándose activamente en ejercicios y pruebas, mediante auditoría de seguimiento y evaluación para la mejora continua.
	Gestionar los ejercicios que se deben desarrollar en el PCN.
	Solicitar los recursos necesarios para las estrategias del PCN.
	Conducir y presentar los resultados de las revisiones para la dirección del PCN.
	Evaluar el impacto de las contingencias que se presenten.
	Efectuar anualmente la revisión del PCN con la actualización del plan estratégico institucional.
	Proponer incorporaciones de eventos disruptivos al PCN al Comité de Continuidad.
	Mantener permanentemente actualizado el PCN.

Tabla 3 Responsable, misión y funciones de Planeación para el PCN
Fuente: Elaboración propia con información del Manual de Funciones de Savia Salud EPS

Desde planeación hay un componente de base para planificar, proponer y conducir desde un posible escenario que hacer ante una amenaza en la continuidad del negocio, a su vez, al ser

responsables del SAR tienen consolidado unos niveles de riesgo que cuentan con medidas de actuación ante la materialización de los mismos y el reconocimiento de las causas para así, mitigar el impacto y cuidar todos los niveles de riesgos a los que se encuentra inmerso Savia Salud EPS.

6.3.4. Tecnología e Información:

Esta dependencia permite el soporte técnico y de seguridad en la organización, y como tal es un proceso fundamental en la continuidad del negocio. A continuación, se presentan el compromiso de la jefatura para definir, crear y diseñar acciones de continuidad y recuperación del estado de normalidad en la operación.

Proceso	Tecnología e información
Responsable	Jefe de Tecnología
Misión del cargo	Dirigir las acciones según lo estipulado en el PCN que implique una respuesta en toda la activación de DRP, y demás acciones para la habilitación de la información necesaria, bases de datos, procesos, Software y Hardware en recurso tecnológico como líder del área de soporte de toda la continuidad de la operación. Además, que se encuentran en el desarrollo del proyecto *Somos +*, el cual será un nuevo aplicativo en reemplazo de integra.
Funciones Específicas	Entregar este manejo a los respectivos responsables sin dejar de ser apoyo y fuente de información para una respuesta adecuada.
	Ser responsable de que todas las actividades se cumplan de acuerdo con lo planeado.
	Diseñar e implementar las estrategias de soporte y monitoreo para brindar soluciones a los requerimientos de los usuarios internos a través de la mesa de ayuda, con criterios de calidad.
	Gestionar la adquisición de recursos para soportar el PCN.
	Proponer incorporaciones de eventos al PCN al Comité de

	Continuidad.
	Participar en el proceso de identificación, medición y control de riesgos operativos relacionados con los procesos críticos que se desarrollan en el PCN y verificar las acciones, tratamientos y controles implementados desde todo lo que tiene que ver con conectividad, seguridad y disponibilidad de la información.
	Asegurar el correcto funcionamiento de los servidores durante los servicios.
	Coordinar las acciones de los grupos de trabajo y la de los proveedores de servicios de red y tecnológicos, como sus recursos internos necesarios para restablecer el servicio en caso se produzca el evento.
	Organizar las acciones necesarias para asegurar un servicio continuo de los servidores y sus aplicaciones.
	Presentar los reportes de la operación contingente al Comité de Continuidad.
	Velar por que el personal a su cargo cumpla de manera oportuna, eficiente y cordial las funciones asignadas para el PCN.

Tabla 4 Responsable, misión y funciones de TI para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo.

Así mismo, la jefatura de TI vela porque cada uno de los procedimientos involucrados en la seguridad de información para los procesos críticos y actividades prioritarias reconocidas por las áreas, deben mostrarse conforme al compromiso que tienen dentro del nivel de ejecución, mitigación y protección; lo anterior puede aportar como medida de acción y entrar en activación al DRP en el momento de presentarse el evento disruptivo, teniendo en cuenta el paso a paso que debe seguir el proceso misional para la identificación de los recursos necesarios que se encuentra a su cargo, según las necesidades tecnológicas que este estipula.

En el mismo orden de ideas, cada uno de los siguientes procedimientos también hace parte del equipo de soporte técnico y de seguridad de la información. De este modo, se ilustra una tabla por cada uno de los procedimientos definidos y las responsabilidades necesarias para cubrir

asuntos como: creación de bases de datos, diseños de software, portadores de Backup, planes de contingencia, construcción del DRP, recuperación de información, entre otros.

Proceso	**Infraestructura y Seguridad Informática**
Responsable	Coordinador de Infraestructura y Seguridad Informática
Jefatura que reporta	Jefe TI
Misión del cargo	Coordinar las actividades técnicas necesarias que garanticen la infraestructura tecnológica y acceso a la misma. Teniendo en cuenta las funciones donde proyecta documentos de carácter técnico, tendientes a mejorar las políticas de uso y seguridad en la red inalámbrica de la entidad. Además de proponer planes, programas y actividades relacionados con la adquisición de tecnología en materia de redes inalámbricas, que cubran y se ajusten a las necesidades y presupuestos de la entidad.
Funciones Específicas	Coordinar las actividades técnicas necesarias que garanticen la disponibilidad de los equipos de usuario final y demás elementos que conforman la red de voz de la entidad.
	Velar por el manejo de incidentes de seguridad en los dispositivos de usuario final.
	Atender oportunamente los requerimientos o incidentes reportados al área de sistemas.
	Evidenciar y actualizar debidamente los documentos técnicos de hojas de vida de los equipos que conforman la infraestructura inalámbrica de tic que reposa en el Data Center.
	Realizar seguimiento a los controles del correcto funcionamiento de la infraestructura por medio de la plataforma de monitoreo con el acompañamiento del proveedor TIGO.
	Activar plan de contingencia en el momento que se presente cualquier indisponibilidad en el servicio de la infraestructura (estado: construcción).

	Orientar la ubicación del procedimiento que da reconocimiento a los funcionarios críticos de la organización.
	Amparar la replicación de información BI a DC alterno.
	Divulgar la estrategia de respaldo integral de solución.
	Disponer de la implementación DA para segmentar el acceso a bases de datos.
	Documentar toda acción según las necesidades del proceso misional, para garantizar la alternativa de red, disponibilidad de equipos, seguridad, entre otros.
	Mantener la separación de roles de bases de datos (core y no core) en infraestructura independiente.
	Infraestructura independiente para ambientes de pruebas, pre y producción.

Tabla 5 Responsable, misión y funciones del proceso de Infraestructura y Seguridad informática para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Proceso	**Arquitectura**
Responsable	Coordinador de Arquitectura
Jefatura que reporta	Jefe TI
Misión del cargo	Encargarse de la creación del producto (aplicativo), siendo así una guía tecnológica para la creación o cambios de los aplicativos, la actualización de lo interno, y como debe dar la solución para el proveedor (los demás procesos), así este interrelaciona los sistemas de información y apoyo tecnológico a las otras coordinaciones de TI. Con un conocimiento técnico para apoyo a otras áreas a partir del software prestando los servicios al área; se garantiza el cumplimiento desde las necesidades del usuario final, las cuales solo son conocidas mediante la información suministrada por los procesos.
Funciones Específicas	Responsable de solución técnica de la continuidad. Contando con salas de atención vital cuando se cae el proceso y hacer las

	validaciones al cliente afectado.
	Llamar al operador en la actualidad TIGO, para desarrollar y diseñar manual y un plan de contingencia que cubra la información misional del proceso afectado, mientras este se soluciona. (Esto se encuentra en un local alterno)
	Visualizar que necesita técnicamente mediante un plan las áreas del negocio.
	Validar y diseñar estrategias de arquitectura del producto para garantizar de lo posible la estabilidad de los servicios.
	Diseñar y crear las mejores condiciones y mediciones con todo el tema de integración entre el sistema de información, sino este trae consigo la no continuidad de la operación.
	Validaciones de la negación del servicio, antes de entrar en alerta.
	Velar que exista seguimiento y garantizar los servidores de conectividad que estén activos.
	Prestar servicio equivale a tener un personal adecuado para continuar operando.
Observación	Desde arquitectura tienen claridad frente a que podría generar una no oportunidad del servicio, la falta de personal de un sistema equivale a esa no continuidad de su proceso, aquí la persona encargada actualmente del proceso maneja como estrategia la rotación constante del personal para no hacer independiente el conocimiento, aunque haya un experto personal para cada producto (control de bases de datos, interoperabilidad, tutelas, entre otros). Tiene la capacidad de brindar una solución temporal o definitiva sin parar la continuidad del proceso.

Tabla 6 Responsable, misión y funciones del proceso de Arquitectura para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Proceso	Software
Responsable	Coordinador de Software
Jefatura que reporta	Jefe TI
Misión del cargo	Garantizar la operación y estabilidad de los sistemas de información de la empresa, y el crecimiento de estos para cumplir con las necesidades del negocio, velando así porque los sistemas de información sean aptos, garantizando la captura y la disponibilidad de la información. Contribuyendo con acciones de mejora que proteja todas las actividades necesarias para operar en el momento de una contingencia.
Funciones Específicas	Participar en el proceso de identificación, medición y control de riesgos operativos y verificar las acciones, tratamientos y controles implementados.
	Reconocer las acciones de mejora que amplíen la estabilidad del proceso en cuanto a la incertidumbre que pueda presentarse.
	Suministrar planes de formación necesaria en el tema de seguridad desde el proceso de software para los requerimientos de la continuidad en la operación.
	Disponibilidad de los sistemas de información mediante los servidores que maneja infraestructura.
	Apoyarse de la acción de contingencia de infraestructura para un evento locativo.
	Apoyarse en el proveedor, mediante lo planeado por las áreas en el contrato.
	Cubrimiento mediante el sistema de toda la información que las áreas necesitan respaldadas.
	Protección a la caída del software dado que trae consigo un gran impacto para el negocio.
	Restablecer en el menor tiempo posible el servicio, si es contratado; ya hay unos acuerdos de niveles de servicios con el proveedor,

	donde este debe garantizar el restablecimiento del servicio - Acuerdo de Niveles de Servicio (ANS).
	Respuesta en un tiempo determinado dependiendo del evento.
	Restaurar aproximadamente en una hora calendario el fallo total del aplicativo integra o bloqueo.
	Recuperar información para los procesos que necesiten luego del PCN activado para volver al sistema u otras alternativas ya definidas.
	Participar de planes de mejoramiento desde su procedimiento para las áreas críticas.
	Plantear evaluación del sistema Integra, proponiendo cambios para el software, como actualmente funciona el proyecto de somos+.
	Valorar sistemas que den cumplimiento a las nuevas necesidades que presenten las áreas.
	Soporte a productos (aplicaciones) que implica procedimientos de los procesos misionales.
	Reorganización de los riesgos desde infraestructura.

Tabla 7 Responsable, misión y funciones del proceso de Software para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Proceso	**Gestión de información y analítica de datos**
Responsable	Coordinador Gestión de información y analítica de datos
Jefatura que reporta	Jefe TI
Misión del cargo	Coordinar el proceso de gestión de información, asegurando que la información vital de la EPS sea veraz a la realidad del negocio; dispone de la participación en la implementación de acciones definidas previamente en los planes de mejoramiento, realizando un seguimiento adecuado de los mismos, para cerciorarse de la mejora continua en los procesos del área. Así como, identificar y proponer a la EPS las necesidades de diseño y mejoramiento de los sistemas integrados de información; lo cual es esencial para propender por el

	diseño e implementación de procedimientos e instrumentos requeridos para mejorar la prestación de servicio sobre toda la información.
Funciones Específicas	Velar por que la información en cuanto a conectividad y bases de datos, que tiene la organización mediante los servidores externos y redundantes; dado que por infraestructura física no hay un impacto al tener la seguridad de la información.
	Disponibilidad de la información en cuanto a seguridad y respaldo de la organización.
	Establecer mecanismos de accesibilidad a esa información para el contexto de contingencias.
	Brindar apoyo en la gestión de información y modelamiento de la información a quien lo requiere. (Bases de datos – modelos cruzados, predictivos, entre otros)
	Proponer estrategias para el diseño de instrumentos de recolección de información, definición de variables y necesidades requeridas por el proceso misional, para el apoyo en la prestación del servicio.
	Disponer con el apoyo de los procesos involucrados, los medios y mecanismos necesarios para transmitir la información a otros niveles del sistema.
	Verificar las acciones de mejora, tratamientos y controles implementados a los riesgos que el proceso tiene identificados que afecta la continuidad de la operación.
	Determinar un plan de contingencia donde se definan actividades a seguir para que el proceso pueda operar mediante otras alternativas.
	Proponer solucionas alternas que desarrollen procedimientos a seguir para la información resguardada y la solicitud de la misma pueda seguir con disponibilidad.

Tabla 8 Responsable, misión y funciones del proceso de Gestión de información y analítica de datos para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Como se evidenció en cada una de las tablas, cada proceso de TI aporta significativamente con actividades necesarias para poder recuperarse a un evento disruptivo, mediante recursos tecnológicos que necesita la organización para continuar con su funcionamiento. El especificar los responsables y las funciones de cada uno de los procesos, define la escala de involucramiento que tienen para apoyar, en la generación de nuevos procedimientos y con ello mejorar el cubrimiento de los procesos críticos.

6.3.5. Prestación en Servicios de Salud:

Es el proceso misional de la organización, por el cual se pueden suministrar todos los servicios solicitados por los afiliados a la EPS, así mismo, en las siguientes tablas se evidencia cómo cada uno de ellos debe tener procedimientos claros, monitoreo y pruebas mediante auditorías, que otorguen garantía de una atención integral e independiente de la sede de prestación y, de la categoría del usuario (régimen subsidiado o contributivo).

Proceso	**Acceso a Servicios de Salud**
Responsable	Director de Acceso
Jefatura que reporta	Subgerencia de Salud
Misión del cargo	Velar por el cumplimiento de las políticas, objetivos, normas, procedimientos y demás actividades establecidas dentro del PCN. Además de tener claridad de los procedimientos que debe seguir llevando acabo luego de un evento disruptivo para la prestación del servicio en salud. Teniendo en cuenta los recursos mínimos, la información habilitada para la operación y todo el proceso a seguir desde el plan de contingencia del área de salud.
Funciones Específicas	Procurar la contratación de la red de salud de acuerdo con las necesidades de la población, basados en el análisis de suficiencia y capacidad de la red ofertada.
	Garantizar la referencia y contra referencia de los afiliados entre los diferentes prestadores luego del evento, a través de un proceso definido como acción activar en cuestión de crisis.
	Mantener el servicio según los criterios y requisitos establecidos en

	la contratación con los proveedores de servicios de salud, medicamentos y tecnologías en salud para la atención de los afiliados.
	Participar en la formulación de estrategias relativas a los procesos en que se involucre el acceso a servicios de salud por parte de los afiliados.
	Facilitar el acceso a los servicios de salud de la población afiliada con criterios de oportunidad y calidad, mediante un proceso de autorizaciones basado en un paso a paso que indique el direccionamiento según el evento, y la habilitación del servicio.
	Detallar el sistema de auditoría integral que vele por la atención de los afiliados con criterios de racionalidad además de un seguimiento continuo a la operación de la red.

Tabla 9 Responsable, misión y funciones de Acceso a Servicios de Salud para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Proceso	**Aseguramiento**
Responsable	Director de Aseguramiento
Jefatura que reporta	Subgerencia de Salud
Misión del cargo	Dar orientación y apoyo a la subgerencia de salud en la formulación, coordinación, ejecución y control de las estrategias de aseguramiento para continuar con las afiliaciones al régimen subsidiado y contributivo y la eficiente administración de las bases de datos, con el fin proteger los ingresos y mantener a los afiliados a pesar de un evento disruptivo.
	Organizar, desarrollar, monitorear y controlar las actividades significativas para mantener el aseguramiento de la población afiliada de los regímenes subsidiado y contributivo.
	Verificar la aplicación de los procesos y procedimientos del control corporativo del aseguramiento de la organización.
	Participar en la formulación estrategias y planes referidos a los

Funciones Específicas	procesos que permiten las afiliaciones y consultar las novedades de afiliados.
	Comprobar las cantidades de afiliaciones realizadas y coordinar la seguridad de la información de acuerdo con los procedimientos establecidos para la prestación del servicio.
	Disponibilidad en la realización del seguimiento, comprobando la integridad y oportunidad de los datos de afiliaciones y novedades en las bases de datos correspondientes.
	Controlar la verificación de los requerimientos internos, de los afiliados, beneficiarios y entes de control en los términos establecidos o acordados luego de la activación del PCN.
	Responder por la actualización correcta y oportuna de los aplicativos y/o funcionamiento manual utilizados en la ejecución de los procesos del área de aseguramiento.
	Detallar de manera integral las bases de datos de aseguramiento para la continuidad del servicio.
	Analizar la información de indicadores de gestión para el diseño de nuevas estrategias o planes correctivos dentro del proceso para la continuidad del mismo.
	Dar respuesta a las auditorias que realiza el Comité de continuidad en cuanto a plan de contingencia.

Tabla 10 Responsable, misión y funciones del proceso de Aseguramiento para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Proceso	**Autorizaciones**
Responsable	Jefe de Autorizaciones
Jefatura que reporta	Subgerencia de Salud
Misión del cargo	Interactuar con el operador en el seguimiento a las políticas y directrices generadas por Savia Salud EPS. Orientado a la gestión de la planeación frente al proceso de autorizaciones y el ajuste del

	modelo para términos de contingencia, donde entra a operar la alternativa elaborada para la continuidad del servicio.
Funciones Específicas	Proponer y diseñar las actividades significativas relacionadas con el proceso.
	Realizar seguimiento al comportamiento de las autorizaciones desde el costo por región teniendo en cuenta como se seguirá operando.
	Monitoreo de pruebas y evaluación del tablero de indicadores.
	Mantener documentado la información frente a la supervisión a los contratos.
	Relacionamiento con instituciones para comunicar qué hacer y qué permitir de manera anticipada en cuestiones de presentarse un evento, además del conducto a seguir frente al mecanismo de las autorizaciones.
	Relacionamiento con alcaldes, directores locales y personeros de municipios según las medidas de emergencia que tengan previstas y que alimentan los riesgos de los procesos críticos.
	Elaborar y realizar seguimiento al guion de direccionamiento del paso a paso a seguir por un tiempo determinado al procedimiento de autorizaciones.
	Definir recursos tecnológicos, físicos y el personal necesario para continuar con el servicio de autorizaciones.
	Definir la comunicación en compañía de la dependencia de Comunicaciones para la atención y respuesta de las quejas de los usuarios.
	Participar en auditorias de control en todo lo relacionado con el proceso de autorizaciones.
	Representación de la organización cuando sea requerido.
	Realizar las evaluaciones de desempeño de las alternativas a usar para continuar con las autorizaciones en los diferentes municipios.

	Diseñar estrategias coyunturales cuando se presentan contingencias.

Tabla 11 Responsable, misión y funciones de autorizaciones para el PCN
Fuente: Elaboración propia con información del manual de funciones y entrevista al responsable del cargo

Cada uno de las anteriores tablas son los encargados del acceso, el aseguramiento y las autorizaciones, necesarios para especificar las medidas de cómo prestar el servicio de salud en cada evento requerido y del equipo humano y técnico que lo compone.

6.3.6. Procesos críticos (Líderes críticos):

Cada área de la organización deberá identificar los cargos que cuentan con procesos críticos que puedan alterar la disponibilidad de las áreas críticas incorporadas como principal y de mayor impacto dentro de este plan. Para realizar esta identificación se debe elaborar un relacionamiento de los procedimientos a cargo que alimenten en cuanto a información, bases de datos, recursos tecnológicos, creación o diseño de indicadores, planes, metodologías, entre otros; no teniendo este relacionamiento identificado, se puede generar un reproceso o una no totalidad de lo que necesite la organización para continuar ofreciendo el servicio.

A continuación se evidencia la estructura del PCN, donde se encuentran los procesos que anteriormente se definieron con sus responsables y sus respectivas funciones dentro de este plan. Los proceso tienen un comportamiento cíclico que reflejan la importancia de cada uno de los responsables para entrar en ejecución el plan, teniendo en cuenta que toda gestión realizada es con el fin de prevenir, atender y mitigar desde su rol correspondiente, asumiendo así el comité de continuidad la última voz de todas las decisiones pertinentes para continuar con la operación.

ESTRUCTURA DEL PLAN DE CONTINUIDAD DEL NEGOCIO

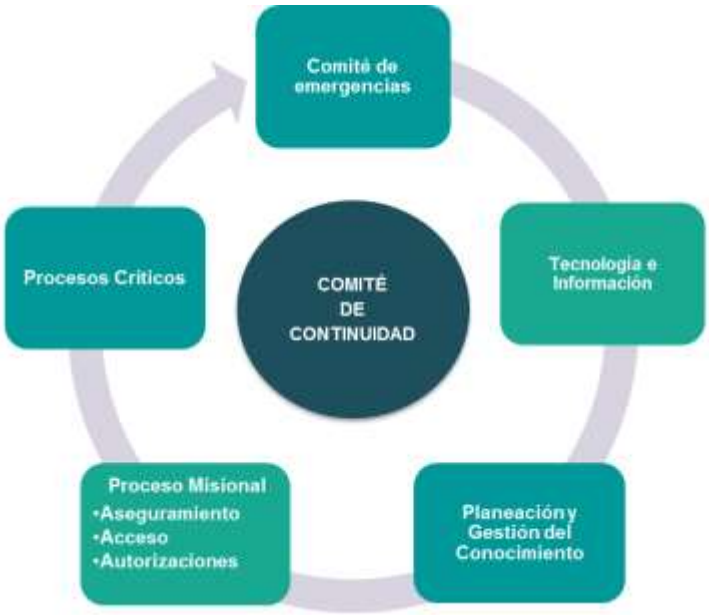


Ilustración 2 Diagrama Responsables del Plan de Continuidad del Negocio
Fuente: Elaboración propia Estructura del PCN basado en la Norma ISO 22301

La relación que se puede interpretar dentro de este diagrama, es que el nivel de acción que cada uno de los actores tiene, es igual de importante durante una planeación, consecución y ejecución del PCN. La flecha indica como todos estos procesos se encuentran en movimiento según las necesidades e indicaciones que el eje central de esta estructura (Comité de Continuidad) requiera para interponer todos los elementos necesarios en el compromiso de la continuidad de la operación durante un evento que irrumpa su normal funcionamiento.

6.4. Recursos

La organización asigna los recursos pertinentes para la difusión, implementación y mejoramiento del PCN, mediante la presentación de una propuesta al Comité de Contratación para su aprobación, lo que permite anudarse al Plan Estratégico Institucional – PEI-; según el escenario proyectado de ocurrencia, los recursos deben ser asignados para capacitación, simulación y/o materialización del evento.

Algunas de las inversiones que debe realizar Savia Salud EPS para la divulgación del PCN, están relacionadas con la sensibilización y capacitación de las personas, así como contratación de servicios tecnológicos, arrendamiento de instalaciones alternas para ejercicios de simulacro y asignación de recursos para la realización de teletrabajo. Adicionalmente, se pueden celebrar convenios con entes públicos que no implican una asignación de recursos económicos, como lo puede representar la utilización de infraestructura física y tecnológica de los socios de la organización como lo son: la Alcaldía de Medellín, la Gobernación de Antioquia y Comfama. Además, de reconocer los contratos que manejan la organización con proveedores como Conexia y Andes BPO que cuentan con su PCN según el servicio que vincule la operación de la entidad.

6.5. Sensibilización y Capacitación

Dentro de Savia Salud EPS, el Comité de Continuidad debe socializar el PCN en los tres meses posteriores a su aprobación, así como integrarlo a la inducción para los nuevos miembros de la organización. Luego debe realizar una jornada de sensibilización una vez al año para toda la organización y si las estrategias definidas traen cambios por nueva insfraestructura o cambio de objetivos deberá actualizarse y socializarse.

Jornada de sensibilización. Se realiza de manera presencial y/o virtual toda la divulgación de la información general, el objetivo del PCN y la política que lo rige, para que así todos los trabajadores sepan la importancia de este plan para la organización.

Jornada de capacitación. Se trabaja desde el plan de comunicaciones a cargo de la dependencia de Comunicaciones Corporativas, desde allí, se direcciona la necesidad de realizar formatos, donde se lleve el registro de los acciones que rigen la capacitación, como pueden ser: ejercicios de pruebas, evaluaciones y seguimiento a las mismas. De esta manera, el Comité de Continuidad ejecuta la approbación de las capacitaciones y sus condiciones; así mismo, las jornadas dan a conocer el rol que tiene cada unos de los empleados dentro del PCN, y las acciones correspondientes para la activación en las jornadas de simulación.

6.6. Comunicación

Las comunicaciones se manejan según el “Plan de prevención, atención y respuesta ante emergencias”- OD-GH-03, mediante la dependencia de Comunicaciones Corporativas, los cuales establecen los protocolos de comunicación interna y externa ante la ocurrencia de un suceso. Divulgando así la información autorizada por Savia Salud EPS y el Comité de Emergencias a las partes interesadas, los trabajadores, afiliados, medios y otros.

En los ejercicios de pruebas del PCN, la dependencia de Comunicaciones Corporativas es la encargada de comunicar a nivel interno y externo los ejercicios de prueba que se efectúen dentro del PCN, usando los canales asignados y reconocidos para divulgar a la hora de realizarse un simulacro o activarse el plan. Las partes externas que son de interés dentro del PCN se encuentran en el documento Anexo. Información General Plan de Emergencias, en la hoja nombrada: Grupos de Apoyo Externos.

6.7. Información documentada

El proceso que se debe llevar a cabo para la formalización de creación de documentos que dan cumplimiento al registro de los procedimientos que se deben ejecutar en el PCN, tiene como objeto poder darle un seguimiento y control frente al impacto que el plan utiliza para el retorno de la operación y su mejora continua.

De acuerdo con el Sistema Integrado de Gestión de Calidad – SIGC de la organización, la dependencia de Gestión de calidad es la encargada de formalizar la codificación para la generación de nuevos documentos como pueden ser: planes de recuperación de procesos, formatos para simulación del PCN, modelo de Nivel de Madurez, entre otros. Con la necesidad de registrar todo aquello que sea necesario para cubrir al máximo el nivel de vulnerabilidad.

Dado lo anterior se especifican los documentos formalizados con los que ya cuenta la organización, que son insumo y parte del PCN:

Inventario de Documentos exitentes

- Plan de Contingencia para Garantizar la Continuidad en la Prestación de los Servicios de Salud – Código OD-RS-08
- Formato acta – Código FO-GC-04
- Plan de Prevención, Atención y Respuesta ante Emergencias – Código OD-GH-03
- Anexo 1 Información General Plan de Emergencias
- Anexo 2 Análisis de Riesgos y Vulnerabilidad
- Anexo 3 PON de evacuación
- Anexo 4 Procedimientos Operativos Normalizados
- Manual de Gestión de Riesgos – Código MA-PN-02
- Matriz de Riesgos – Código FO-PN-05
- Plan estratégico de tecnologías de la información y comunicación – Código OD-TI-07

De acuerdo con lo mencionado, se enlista a continuación los documentos que luego de aprobar el PCN por el Comité de Continuidad, estos deben tenerse en cuenta para empezar todo el proceso de aplicación y ejecución según lo designado por la organización:

Inventario de Documentos por formalizar

- Acta creación Comité de Continuidad
- Plan de Continuidad del Negocio
- Plan de Recuperación de Procesos Aseguramiento
- Plan de Recuperación de Procesos Acceso
- Plan de Recuperación de Procesos Autorizaciones
- DRP – Plan de Recuperación Tecnológica
- Formato de Nivel de Madurez - Herramienta de medición de la Gestión organizacional
- Herramienta BIA- Analisis del Impacto del Negocio
- Identificación de recursos necesarios para el PCN

Dentro de este contexto una vez se creen y formalicen los documentos, este será divulgado parcialmente a las partes interesadas, a través de capacitaciones y simulacros, donde se da a conocer elementos del PCN teniendo en cuenta los roles y el grado de involucramiento de las

partes interesadas, dado que a nivel estratégico se considera un documento clasificado con acceso restringido.

Cabe concluir que el PCN, se actualiza una vez al año o cada vez que se incluyan nuevos procesos en el alcance y/o se realicen cambios considerables en la organización, esto debe formalizarse mediante realización de actas dentro del Comité de Continuidad, donde quedan estipulados los compromisos, los cambios y los responsables de esta integración para así pasar a ser actualizado por la dependencia de Planeación y Gestión del Conocimiento. Estos cambios se socializan con las partes interesadas durante el desarrollo del plan de capacitaciones anuales y/o cuando se requiera por actualización del documento.

7. OPERACIÓN

Para la ejecución del PCN de Savia Salud EPS, se utiliza la estrategia administrativa del ciclo planear, hacer, verificar y actuar (PHVA) que permite la mejora continua del plan; a su vez como marco de referencia para su formulación, además de tener como referente la Norma ISO 22301 de 2012 como guía en el manejo de la estructura de dicho plan.

Sumado a ello, para la realización del análisis situacional de la organización en términos de la continuidad del negocio, se efectúan entrevistas y reuniones con personas encargadas de los procesos necesarios para reconocer las acciones de prevención, atención y mitigación a los eventos de emergencia; también, se revisa y recopila la información pertinente que sirve como componentes y acciones complementarias del PCN.

Adicionalmente, es importante expresar que, en dichas reuniones con los respectivos líderes de los procesos críticos, se conocen necesidades, expectativas, requerimientos, recursos, tiempo máximo permitido sin operación, entre otros aspectos necesarios para el análisis del impacto del negocio. Según el alcance propuesto se hace ineludible en el verificar y actuar, que una vez aprobado el PCN se establezca un inventario de riesgos de alto y mediano impacto, realizar seguimiento y control mediante ejercicios de pruebas, auditorias y definición de indicadores, los cuales permiten saber el desempeño del PCN; de acuerdo a los resultados del seguimiento (a partir de que resultado se presenta el plan de mejora) se debe implementar planes de mejora, para la retroalimentación y el mejoramiento continuo del mismo.
En la siguiente ilustración se puede observar el ciclo PHVA para la gestión del PCN en Savia Salud EPS:

Ilustración 3 Ciclo PHVA
Fuente: Elaboración propia basada en la Norma ISO 22301

El desarrollo del PCN también se fundamenta en las siguientes diez etapas que se pueden ver en la siguiente tabla, tomada de (APEC, 2014) como pautas donde se determina de manera operativa la importancia y el cumplimiento de formular el alcance, las actividades prioritarias, la evaluación de riesgos y las demás que se encuentran enunciadas de manera ascendente, aportando en la formulación del plan y en la mejora continua del mismo.

10 pasos para desarrollar el Plan de Continuidad de Negocios	
Paso 1	Determinar el Propósito y alcance de tu PCN y selecciona al líder y equipo responsable de llevarlo cabo
Paso 2	Determinar las Actividades Prioritarias de la empresa y los Tiempos de Recuperación Ideales
Paso 3	Determinar qué se necesita para la continuidad del Negocio
Paso 4	Evaluación de Riesgos - Conozca sus escenarios de riesgo.
Paso 5	No olvidar protección previa al desastre y métodos de mitigación

Paso 6	Respuesta de Emergencia ante el desastre
Paso 7	Estrategias para Continuidad de Negocios Temprana
Paso 8	Estar preparado financieramente
Paso 9	La práctica hace que el plan sea funcional
Paso 10	Revisión continua y mejoramiento del Plan

Tabla 12 Etapas para desarrollar el PCN
Fuente: APEC MSME Market Place – Guía para desarrollar un PCN

Por medio de la continuidad del negocio, se busca el desarrollo de la capacidad estratégica, táctica y operativa de la organización, para responder a eventos adversos que puedan ocasionar altos impactos y amenazar la continuidad y sostenibilidad de la entidad, para ello se realiza un modelo de actuación donde ilustra la relación que tienen las acciones desarrolladas en Savia Salud EPS y la continuidad del negocio. Como se ha podido evidenciar a lo largo del documento, un asunto transversal e importante en el mismo es el tema de los *riesgos*. Estos se pueden clasificar en:

Riesgos de Alto Impacto. Representa una situación de emergencia, siendo aquellos factores internos y externos que influyen directamente en la continuidad de la operación de la organización y que intervienen en casos de incendio, ataque terrorista, un hacker en el sistema, desastre natural entre otros; este requiere de acciones inmediatas donde se activará del PCN para este caso.

Riesgos de Mediano Impacto. Aquellos riesgos consignados en el SAR, que tiene un impacto parcial a las actividades que realiza cada proceso de la organización, lo cual no genera un riesgo de pérdida total, y tiene unas acciones preventivas y correctivas para mitigar su materialización, además de llevar a cabo controles temporales enfocados a la efectividad operativa y la protección de los sistemas.

Riesgos de bajo impacto. La amenaza aquí no representa un evento que impacte a los procesos para realizar acciones para activar el PCN, dado que puede disponer la atención y reducción de manera paralela con otras mejoras operativas.

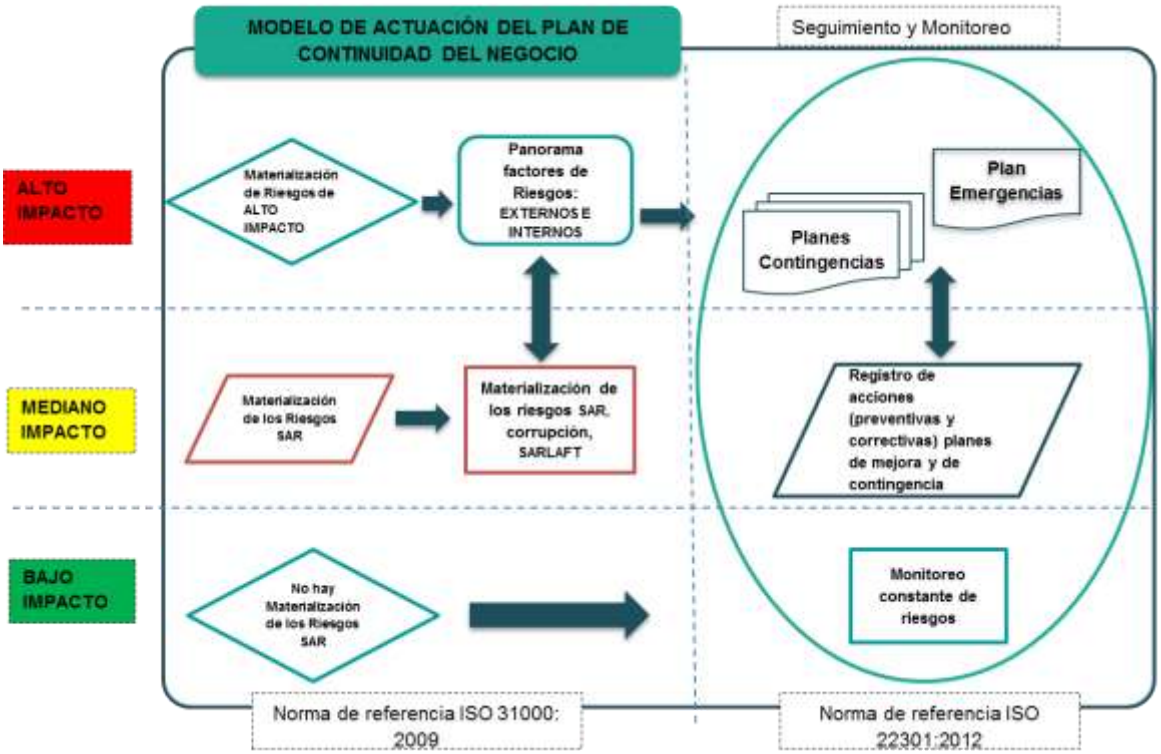


Ilustración 4 Modelo de actuación del Plan de Continuidad del Negocio
Fuente: Elaboración propia basado en el esquema metodológico del SAR de Savia Salud EPS

Según la ilustración del "Modelo de Actuación del Plan de Continuidad del Negocio" lo que se busca es establecer el nivel de riesgo e impacto ya sean por factores internos o externos, y definir un modelo de actuación que permita dar metodológicamente una forma de desarrollar y orientar las acciones a realizar; en caso de materialización del riesgo ya sea de alto, medio o bajo impacto.

Para la materialización del riesgo de ***Alto Impacto*** se tendrá en cuenta el panorama de factores de riesgos definidos por la organización, y los riesgos definidos en el sistema de administración de riesgos SAR como altos; para ello se tendrá como modo de actuación los planes de contingencia, de emergencias y desastres de acuerdo al tipo de amenaza, evento o vulnerabilidad de Savia Salud EPS. Para el nivel de ***Mediano Impacto***, se tendrá en cuenta las mismas acciones de acuerdo al nivel de riesgo y esto se complementa con la Matriz de Riesgos de Corrupción y SARLAFT. A su vez, para un nivel de ***bajo impacto*** se hará el monitoreo y seguimiento constante.

Este modelo de actuación se hace con el fin de dar respuesta de manera estratégica, táctica y operativa, poder articular todos los planes mencionados técnica y metodológicamente y, ajustados a las Normas ISO/ HSEQ.

De acuerdo con lo anterior, se hace necesario listar todos los planes de contingencias de las áreas críticas de Savia Salud EPS dado que en ellos se identifican los riesgos de alto y mediano impacto para definir las necesidades y los apoyos necesarios para darle continuidad al negocio. Estos se encuentran enunciados en información documentada dentro de este plan, lo cual hace también parte de la revisión de creación de nuevos documentos, planes, formatos, entre otros.

7.1. Desarrollo del Plan de Continuidad del Negocio

En este punto se lleva acabo el desarrollo del PCN, el cual consiste de una herramienta para el análisis del impacto, la estrategia que la organización debe alinear con la continuidad de la operación teniendo en cuenta seis acciones que se deben realizar en el periodo de tiempo que la coyuntura lo requiera. Así mismo, se anudará los procesos de recuperación tanto para el área misional, como el proceso de apoyo Gestión TI con su DRP, Dando por terminado con las especificaciones para retornar la normalidad de la operación.

7.1.1. Análisis del Impacto del Negocio – BIA

El Análisis de Impacto al Negocio – BIA (Business Impact Analysis), se desarrolla con el fin de identificar el tiempo máximo fuera de operación, el nivel de criticidad y la priorización de los diferentes procesos de la entidad; todo esto se hace mediante la revisión de los impactos financieros, operacionales, legales y de imagen corporativa, que afectan a Savia Salud EPS en caso de presentarse un evento negativo; para el levantamiento de esta información, es necesaria la realización de entrevistas a responsables de los diferentes procesos considerados como críticos.

Al explorar las consecuencias de la interrupción de los servicios, se evidencia que en lo operacional y financiero hay altos impactos, así estos se consideran de alta criticidad, siendo

estos en su inicio el proceso misional que representa las tres áreas de salud: Acceso, Aseguramiento y Autorizaciones y, el proceso de apoyo: Gestión de TI, se expone así un tiempo máximo donde cada proceso puede estar en estado de no operación y además los recursos mínimos que necesita para la recuperación de la misma interrupción.

Por su parte, para definir el nivel de criticidad de cada uno de los procesos, se aplica el siguiente método de calificación desde la interpretación del proceso que se está valorando para la entidad.

Nivel de Criticidad	
Valor	**Interpretación del proceso crítico**
Alto	Crítico para el Negocio, la función del negocio no puede realizarse. No puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas.
Moderado	No es crítico para el negocio, pero la operación es una parte integral del mismo. No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles y este puede sustituirse temporalmente por un proceso manual.
Bajo	La operación no es parte integral del negocio. Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles, y sustituirse parcialmente por un período, por un proceso manual.

Tabla 13 Método de calificación nivel de criticidad
Fuente: Elaboración propia con información del Manual de Gestión de Riesgos de Savia Salud EPS

A través de este método, se determina la asignación de recursos mínimos, la mayor atención y seguridad de los procesos interrumpidos, teniendo en cuenta el tiempo máximo que estos pueden soportar fuera de servicio y así llevar un reporte de los hallazgos encontrados.

Por consiguiente, la siguiente tabla evidencia la aplicación del método para determinar la calificación de los procesos críticos seleccionados por la organización, teniendo así un mapeo de cubrimiento debe de tenerse en cuenta, según el nivel de criticidad, los sistemas de información y las instalaciones.

Proceso Crítico	Sistema de Información		Instalaciones	Tiempo máximo fuera de servicios
	Software (Conexia)	Hardware (Tigo)		
Sistema de Información y conectividad	X	X	X	2 horas
Autorizaciones de servicios	X	X	X	24 Horas
Afiliaciones	X	X	X	48 Horas
Prestación de servicios en sedes	X	X	X	24 Horas
Central de referencia y contrarreferencia	X	X	X	4 horas

Tabla 14 Nivel de Criticidad procesos críticos
Fuente: Elaborado por la dependencia de Planeación y Gestión del conocimiento basado en la Norma ISO 22301

Cada uno de los procesos recibe una calificación en cuanto a sistema de información, instalaciones y el tiempo máximo fuera de servicios. Reconociendo los de color rojo como aquellos que no permiten el normal funcionamiento de la entidad, así mismo, para los de color naranja, dado que son una parte integral de la operación; lo cual no avala recursos para continuar con las funciones en la garantía del servicio de autorizaciones a los afiliados. Por último, para los de color verde, evidencia en la tabla que, las instalaciones para la realización de afiliaciones pueden seguir operando de manera manual al no contar con las instalaciones que están destinadas para el proceso.

Luego de determinar cuáles son estos procesos críticos y su nivel de criticidad se tienen unas actividades prioritarias para el proceso misional y el proceso de TI; así mismo, esta se debe calificar con un nivel de prioridad y criticidad, la cual es definida por cada uno de los miembros de los procesos en mención.

Actividades prioritarias del proceso misional: revisando los procesos de la empresa y en entrevista con los responsables de algunos de ellos se encuentra que las actividades prioritarias que se deben garantizar en caso que se produzca una interrupción de la operación son:

Prioridad 1

- Sistema de Información y conectividad
- Autorizaciones de servicios
- Afiliaciones

Luego están otros procesos y/o actividades que estarían en un segundo plano y sobre las cuales es necesario garantizar su pronto restablecimiento:

Prioridad 2

- Transporte de pacientes
- Prestación de servicios en sedes.
- Central de referencia y contrarreferencia.

Actividades prioritarias de Gestión de TI: en la prioridad están definidos según los factores críticos de interrupción al servicio, pudiendo así comprender las pérdidas que puede involucrar la suspensión parcial o total de estas actividades. Garantizando su restablecimiento según el nivel de prioridad. Recordando así que Conexa es quién hoy se encuentra con todo el proceso de aplicativo misional llamado *Somos +* define de la siguiente manera la prioridad

Prioridad 1

- Todos los sistemas vitales de la organización. Corresponde a todos los componentes que conforman toda la solución de *Somos+* de Savia Salud EPS, que en el caso de no ser adaptados oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar la actividad de los clientes.
- Software Aplicativo
- Hardware

Prioridad 2

- Sistemas con múltiples interfaces.
- Sistemas o dispositivos que no pueden ser sometidos a pruebas.
- Sistemas que alimentan datos a los sistemas vitales.

Se le asigna a todos los componentes que conformen la solución de *Somos+* de savia Salud E.P.S, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de control, cuentan con procedimientos alternativos preestablecidos.

Prioridad 3

Sistemas cuya falla causa molestias menores. Se le asigna a todos los componentes que conformen la solución de Somos+ de savia Salud E.P.S, cuya falta de adaptación no representa graves traumatismos y sus modificaciones pueden aplazarse para la última parte del proyecto.

El BIA además ayuda aumentar su cobertura aproximadamente una vez al año, para así; luego de implementado y aprobado el PCN con sus procesos críticos, este puede tener una cobertura total de continuidad de la operación para todos los procesos de la organización. Para ello, las actividades prioritarias deben de establecerse la formulación de un objetivo para continuidad del negocio, los recursos mínimos requeridos para dar cumplimiento a ese objetivo en cuanto a tecnológicos y físicos; así como el personal mínimo para seguir con la operación.

Para recoger la información frente a los recursos mínimos y el objetivo de continuidad del proceso, fue necesario citar a cada uno de los líderes de los procesos críticos de Savia Salud EPS, donde se determina un mínimo de requerimientos para continuar en funcionamiento el proceso, para determinarlos se utiliza una encuesta anexa a este documento, que ayuda a dar un rumbo de determinación en escenarios de amenazas al que se esté expuesta la organización mencionadas en el análisis situacional.

Nº	Proceso Crítico	Objetivo para la continuidad de negocio	Recursos mínimos requeridos para cumplimiento del Objetivo			Observaciones
			Tecnológicos	Físicos	Humanos	
1	Sistema de información y conectividad	Plantear y dotar a COMEXA, de los procedimientos y elementos mínimos requeridos para afrontar la contingencia relacionada con el eventual cese de actividades, inoperatividad de equipos causada por razones de fuerza mayor.	*Estaciones de trabajo(laptops y PC s) o impresoras, fotocopiadoras, scanner o Equipos multimedia *Aplicativos alternos *Software de Aplicaciones (WebLogic, Tomcat Apache) o Software Base (Sistemas operativos y Ofimática) • Antivirus para protección de servidores y estaciones de trabajo • Respaldos de información y configuración de los Servidores • Equipos diversos o Grupo Electrógeno o UPS o Aire Acondicionado	• Suministro de Energía Eléctrica. *Servicios Públicos • Servicio de Telefonía Fija analógico/digital y móvil. •Infraestructura para operar, mientras el data center alterno respalda la operación	Disponibilidad de personal de dirección : 4 coordinadores, 1 jefe • Disponibilidad de personal operativo: 2 personas x proceso de cada coordinador	Se encuentra en desarrollo el DRP, que genera todo el cubrimiento tecnológico y de seguridad informática para la organización
2	Autorizaciones de servicios	Establecer las directrices para atender de manera oportuna las contingencias presentadas en la red que conforma la EPS Savia Salud en los diferentes Municipios donde hace presencia, con el fin de coordinar, movilizar y generar los mecanismos necesarios ante la ocurrencia de un evento no planificado que interfiera en la prestación de los servicio de salud.	*Virus informático; de manera masiva, a esta contingencia que respaldo les tiene la dependencia de TI para solucionar este proceso - Aplicativo para el proceso mínimo. *Habilitar URL en las cajas de los autorizadores. *Equipo por persona y habilitados al sistema y red (Internet). *Seguridad alterna para el aplicativo integra dado que hasta ahora se realiza de forma manual *cuarto de datos para tener la información. *chat interno de comunicación	*Infraestructura locativa, Si es solo en 1 una sede, las autorizaciones lo pueden hacer en otra sede. *Las autorizaciones se pueden realizar desde la casa (los encargados) *Conectividad, red y energía que necesita las autorizadores desde el hogar (teletrabajo) **teléfono	1 jefe de área 1 Coordinador Autorizaciones: 20	Las oficinas donde se realiza ambos procesos autorizaciones y atención al público son: Uraba, Rio Negro, Bello, Elite, Girardota.
3	Afiliaciones	Garantizar que el proceso de aseguramiento de la población afiliada en el régimen subsidiado y contributivo pueda recibir el servicio de salud.	*15 procedimientos: Todos los procesos específicos se manejan desde el aplicativo. *Establecer la forma de avisar a los usuarios (medios masivos) *Aplicativo para la atención, para las afiliaciones. *Base de datos de Afiliación y novedades. * Manual- creación de formatos (formulario) *Diseño software con base de datos (ejemplo Access, Click) - licencia del Software municipios que se realiza- básico: (sistema: verificación derechos: centro regulador como propuesta; telefónica *Contingencia del régimen consorcio contractualmente es valido. *Aplicativo local datos mínimos de la afiliación definiendo las variables mínimas. *Atención del usuario: laborar como base corte de mes anterior aplicativo validación, corrección o afiliación con datos básicos para almacenamiento *Reporte Saheduc: norma establecido manual, bases de datos (soporte que se daría para el resto de las de salud para autorizaciones y acceso) acorte del momento o día anterior, procesos y procedimientos: cumplimiento de norma. *gestión documental se conserve de manera digital – como lo son Formulario de afiliación y bases de datos. *Equipos por persona mínima para el proceso.	*Infraestructura alterna, depende de la sede donde se sigue operando. *Impresora Capacidad para las 15 personas: *Escritorios *Sillas *Papelería	15 personas: 1 Jefe afiliaciones 1 Coordinadora de subregiones 1 Jefe área 1 Enfermera Medicina Laboral 4 Analistas 4 Auxiliares de Operaciones 3 Auxiliares de Aseguramiento	Para los procesos es continuo no pueden parar por ende externos algunos procesos. La no operación puede incurrir en Multas, Pagos, Usuario muerte por parecer inactivo, entre otros. Bases de datos (soporte que se daría para el resto de los procesos de salud para autorizaciones y acceso)
4	Prestación de servicios en sedes	Establecer las directrices para atender de manera oportuna las contingencias presentadas en la red que conforma la EPS Savia Salud en los diferentes Municipios donde hace presencia, con el fin de coordinar, movilizar y generar los mecanismos necesarios ante la ocurrencia de un evento no planificado que interfiera en la prestación de los servicio de salud.	*Virus informático; de manera masiva, a esta contingencia que respaldo les tiene la dependencia de TI para solucionar este proceso. *Equipos para atención en salas recibir documentación y guardarla con id y teléfono de contacto, se le puede recibir la documento desde el hospital. (48 horas recibir al información) *Seguridad, con el aplicativo de integra nada se realiza de forma manual - cuarto de datos para tener la información	*Puesto de trabajo por persona. *Sala para gestores ubicada en Medellín.	1 jefe de área (la misma persona del proceso de autorizaciones de servicios) 1 coordinador (la misma persona del proceso de autorizaciones de servicios) Gestores de sala: 40	Las oficinas donde se realiza ambos procesos autorizaciones y atención al público son: Uraba, Rio Negro, Bello, Elite, Girardota.
5	Central de referencia y contrarreferencia	Mantener el contacto con las IPS para el proceso de regulación y referenciación de pacientes.	*Suministro de equipos y la conectividad a través de internet , Estabilidad en la plataforma de Savia Salud (Conexia-Integra) *Web services validaciones automáticas – atención de urgencias (prioritaria) para la validación de derechos y directas a través de los asesores. (Aux. enfermería) *Seguridad de la información en cuarto de datos para todo el proceso de centro regulador. *Conexiones desde las casas de los encargados así evitar el desplazamiento. (teniendo en cuenta la integración del equipo (interconexión reuniones por medio de la red – video llamadas)	*Se tiene alternativa de Sede rio negro o la casa para instalarse mediante operador Andes BPO- estipulado en el contrato (renovación con esta condición) *Toda la infraestructura la tienen en disponibilidad para ellos. (traslado del personal, todo la operación para traslado)	12 personas: 1 Coordinador (a) centro regulador 8 Auxiliares de enfermería 1 Supervisor (a) técnica operativa 1 Médico 1 Ingeniero de soporte (suministra al operador de tecnología e infraestructura).	Documentos relevantes para la continuidad del proceso: Matriz de contingencia, contrato con el operador en mención, plan de contingencia.

Tabla 15 Objetivo y recursos mínimos de operación de los procesos críticos (Anexo de Excel)
Fuente: Elaboración propia con la dependencia de Planeación y Gestión del Conocimiento

Como se evidencia en la tabla 15, este también se anexa a este documento en formato Excel con el nombre de “Recursos necesarios para la continuidad del proceso crítico”, cada proceso en compañía de la dependencia de Planeación y Gestión del Conocimiento realiza la creación del objetivo y los recursos que considera necesarios, con ellos, se podrá proveer en la estructura de recuperación de procesos, el cual debe ir dentro del Plan de Contingencia de cada proceso de la organización. Dado que esto es el inicio de acciones a llevar a cabo durante el evento disruptivo.

Riesgos que pueden afectar la continuidad del negocio: al detallar los métodos que tiene la organización para identificar los factores de riesgos que pueden generar interrupción sobre los procesos críticos, se documentan dentro del plan los que la organización ya tiene identificados mediante las siguientes herramientas: Matriz de Riesgos y Tipos de Amenazas.

Savia Salud EPS al contar con la Matriz de Riesgos usan la metodología de gestión de riesgos del SAR, orientados a anticipar los eventos y la materialización de los riesgos. Esta matriz indica los riesgos a los que se encuentra la organización expuesta en momentos de incidente, así para los procesos críticos nos muestra el tipo de riesgo que tienen cada uno, contando para el proceso misional con un total de diecisiete riesgos, con categoría de riesgo operacional y de salud, su nivel de riesgo inherente siendo ocho en nivel alto impacto y nueve, en moderado impacto.

Riesgos proceso misional:

Actividad significativa (proceso)	Nombre del Riesgo	Nivel de Riesgo Inherente
Gestión del Aseguramiento	Perdida de afiliados	Alto
Gestión de acceso a servicios de salud	No tener red contratada	Alto
Gestión de acceso a servicios de salud	Falta de gobernabilidad sobre la red	Alto
Gestión de acceso a servicios de salud	Inadecuada negociación de servicios y tarifas con los prestadores	Moderado
Gestión de acceso a servicios de salud	Sobre ejecución de los contratos - Centro Regulador	Moderado

Gestión de acceso a servicios de salud	Entrega incompleta e inoportuna de los tratamientos terapéuticos de la población afiliada	Alto
Gestión de acceso a servicios de salud	Inadecuada supervisión de contratos de proveedores, medicamentos, dispositivos médicos e insumos	Alto
Gestión de acceso a servicios de salud	Inadecuada parametrización de productos farmacéuticos	Alto
Gestión de acceso a servicios de salud	Inadecuado seguimiento a productos farmacéuticos	Alto
Gestión de acceso a servicios de salud	Error en la ejecución del proceso - CR	Moderado
Gestión de acceso a servicios de salud	Autonomía para definir prestadores y tarifas	Moderado
Gestión de acceso a servicios de salud	Error en la autorización de los servicios solicitados	Moderado
Gestión de acceso a servicios de salud	Fraude en la emisión de las autorizaciones – CR	Moderado
Gestión de acceso a servicios de salud	Sobrecostos – CR	Moderado
Gestión de acceso a servicios de salud	Suplantación de afiliados – CR	Moderado
Gestión de acceso a servicios de salud	Incumplimiento de los criterios de habilitación de las IPS contratadas (Red de prestadores)	Moderado
Gestión de acceso a servicios de salud	Inadecuado seguimiento en la supervisión de contratos	Alto

Tabla 16 Riesgos de Alto y Mediano Impacto del Proceso Misional
Fuente: Elaboración tabla con datos de Matriz de Riesgos Savia Salud EPS

Al proceso misional tener el reconocimiento de estos riesgos, las causas y consecuencias, la definición de acción preventivas y la valoración de los controles que se realizan, ayuda a tener un registro que sirve para mitigar los impactos de ocurrencia, así como la matriz también nos suministra cada una de las acciones de contingencia que se tienen o deben realizar ante la posible materialización del mismo. Lo que se busca al tenerlas en el PCN, es que se crea, verifique y actualice el plan de contingencia del proceso crítico. Esto trae consigo un reajuste consecutivo y una caracterización de nuevos riesgos que se puedan encontrar, para los cuales se deberá crear medidas y procedimientos para prevenir el mayor porcentaje de perdida frente a la materialización del mismo.

Riesgos proceso de apoyo Tecnología e Información:

Actividad significativa (proceso)	Nombre del Riesgo	Nivel de Riesgo Inherente
Gestión tecnología	Continuidad de la operación	Alto
Gestión tecnología	Integralidad del Sistema de Información (Gestión de cambio)	Alto
Gestión tecnología	Seguridad de la información	Moderado

Tabla 17 Riesgos de Alto y Mediano Impacto del Proceso de apoyo – TI
Fuente: Elaboración tabla con datos de Matriz de Riesgos Savia Salud EPS

Como se observa para el proceso de apoyo de Gestión de TI la continuidad de la operación, la integralidad y la seguridad de la información. Son los riesgos de mayor nivel a los cuales debe protegerse y mitigar su impacto, para ello, se hace necesario saber que tan vulnerable es el acceso, los controles que se tiene frente a una caída en el aplicativo, dado que traen consigo la no generación de autorizaciones, fallas en las bases de datos, perdida de información, limitación del almacenamiento, entre otros. Debido a estos escenarios, es que el DRP puede generar una alta disponibilidad de todos estos procesos críticos teniendo una mayor seguridad y protección con lo que el proyecto ***Somos +*** al rediseñar el Data Center y realizar todos los cambios necesarios para poder continuar con la operación.

Así mismo, de forma institucional se presenta en la siguiente tabla (18) los riesgos externos que la organización tiene identificados, siendo estas categorizadas según el tipo de riesgo, y el impacto que puedan presentarse según el evento, es necesario conocerlas e identificarlas dado que se deben atender en cada plan de recuperación de procesos críticos, para luego tener una cobertura de cada uno de los procesos de la organización en cuanto a las contingencias y sus consecuencias si llegase a materializarse dicha amenaza.

TIPOS DE AMENAZAS	
RIESGO NATURAL BIOLÓGICO	**RIESGOS ANTRÓPICO TECNOLÓGICOS**
Brote de enfermedades	Incendios
Infesta de animales, insectos o plagas	Explosión

RIESGO NATURAL FÍSICO GEOLÓGICO	Fallas en las estructuras
Sismo o terremoto	Fallas en los sistemas y procesos
Licuación de suelos	Accidente de transporte
Deslizamientos	Obstáculos en las rutas de evacuación
Avalancha	Contaminación de alimentos
RIESGOS NATURALES FÍSICO METEOROLÓGICOS	Accidente laboral
Inundaciones	**RIESGOS ANTRÓPICO AMBIENTAL**
Vendavales	Derrame
Tormentas o rayos	Vertimiento
Vientos huracanados	Fugas
RIESGOS ANTRÓPICO SOCIALES	Mezcla de productos químicos o sustancias peligrosas
Terrorismo	Acumulación de residuos sólidos y/o desechos tóxicos
Asonadas	Desertificación - degradación del suelo
Hostigamiento	Deforestación
	Pérdida de biodiversidad
Actividades criminales	Acumulación de material particulado
	Contaminación radioactiva

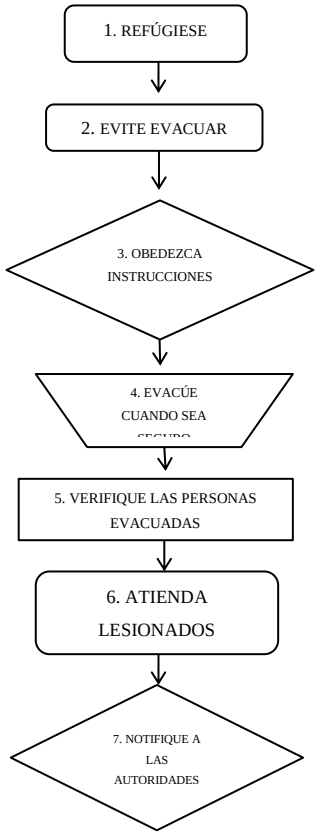
Tabla 18 . Tipos de Amenazas Externas a las que está expuesta la organización
Fuente: Elaboración con datos del Análisis de Riesgos y Vulnerabilidad – Savia Salud EPS

Para cada una de las amenazas se cuenta con un proceso de acción, llamado Procedimientos Operativos Normalizados – PON, previamente definidas las situaciones de emergencia según su calificación que generan un alto riesgo para la organización. Crea acciones establecidas mediante un grupo de líderes que luego de ser aprobadas para preservar ante la ocurrencia de un evento las siguientes características:

- Optimizar el uso de los recursos
- Facilitar las comunicaciones
- Disminuir el nivel de incertidumbre

- Posibilitar una adecuada coordinación

Este procedimiento busca que todas las personas, incluyendo la estructura operativa y administrativa del plan de emergencias y todo el personal en general, estén preparadas para la atención de situaciones de emergencia, teniendo en cuenta acciones de prevención, preparación, atención y recuperación. A continuación, se presenta el flujograma con el que hoy la organización define el paso a paso; según el grado de emergencia, de las acciones que debe realizar acatando las actividades prioritarias de los procesos críticos para accionar su plan de contingencia.

TIPO DE AMENAZA – SOCIAL		
FLUJOGRAMA	**DESCRIPCION**	**RESPONSABLE**
	1. Refúgiese, aléjese de los disturbios, busque un lugar cerca del área donde se encuentra que le brinde la protección adecuada, si no es posible, acuéstese en el suelo.	Todo el Personal
	2. Permanezca dentro de las instalaciones de la empresa.	Todo el Personal
	3. Si recibe órdenes directas de los atacantes, acátelas. No intente nada heroico.	Todo el Personal
	4. Espere la señal de que el peligro ya paso. Recuerde que puede demorarse un buen rato para escuchar esta señal. Espere la orden de evacuación y diríjase al punto de reunión final.	Todo el Personal
	5. Verifique las personas evacuadas al punto de encuentro.	Coord. Evacuación
	6. Inicie la atención de lesionados.	Brigada

	7. Notifique a las autoridades	Comité de emergencias

Tabla 19 Ejemplo procedimiento según tipo de amenaza para los procesos críticos
Fuente: PON anexo 4 del Plan de prevención, atención y respuesta ante emergencias

Según el flujograma que se ilustra anteriormente cada proceso debe contar dentro de su plan de recuperación de procesos con un flujograma que le permita tener una ruta a seguir en caso de verse vulnerable ante el tipo de amenazas externas mencionadas anteriormente, según la prioridad de la actividad, es que se define los responsables, los recursos y quienes externamente deben intervenir en llegar a la normalidad de la prestación de los servicios. Para ello se cuenta con un listado "Grupo de apoyo externo" donde se encuentran las líneas de atención de emergencias en el anexo 1 "Información General de Plan de Emergencias" del Plan de prevención, atención y respuesta ante emergencias.

7.1.2. Estrategia de Continuidad del Negocio

La organización establece como estrategia de apoyo a la *Continuidad del Negocio*, la integración de los planes formulados y puestos en marcha que contienen las acciones, actividades, y personas a cargo de cómo ejecutar el plan según el evento de emergencia que se presente, así como proponer la creación de planes necesarios para prevenir, atender y mitigar la interrupción en la normal operación. Este documento pretende ofrecer una conducta a seguir para la administración adecuada de información, acciones y procedimientos necesarios para facilitar la recuperación ante una disruptiva, donde se cumple los requerimientos que se presentan en la política del PCN y en paralelo con los objetivos de Savia Salud EPS.

Mediante el BIA se trazan los objetivos de continuidad para cada proceso, así como las necesidades de recursos mínimos físicos, tecnológicos y de personal: El BIA también sirve como guía, suministrando una ruta de las pautas necesarias para la creación de los planes que se deben tener en cuenta según el proceso crítico.

Estos planes vistos como parte de la estrategia el PCN, se activan según sea la necesidad, el tipo de evento materializado, las personas afectadas, la infraestructura física y tecnológica impactada y el nivel del riesgo medido; teniendo en cuenta que el PCN es para los desastres

ya mencionados en el análisis situacional donde la continuidad de la operación se vea amenazada; el plan de recuperación de procesos, entra a operar para cada uno de los procesos críticos y si este es un evento que perjudique los sistemas de información, se activarán las estrategias relacionadas al plan de recuperación tecnológico – DRP.

Así mismo, el PCN de Savia Salud EPS debe contar con unos periodos de tiempo para realizar acciones antes, durante y después de entrar en ejecución y poder llegar activarse el plan según el evento o la emergencia para luego alcanzar un estado de normalidad, como se describe a continuación:

1. ***Respuesta inicial y notificación:*** generar una novedad preliminar frente al evento que debe ser preparado como una respuesta inmediata a la interrupción.
2. ***Evaluación del problema y escalamiento del mismo:*** informe del evento debe ser preparado luego de una exhaustiva inspección del sitio.
3. ***Posibilidad de declaración de desastre:*** se hace un reporte del detalle del problema, luego de ser revisado y se toma una decisión y es si se debe o no declarar como desastre.
4. ***Plan o planes a implementar:*** se refiere a los procedimientos necesarios para ser ejecutados y preparación del espacio físico, gestión de los equipos y recursos para la recuperación, reanudación y normalización del servicio.
5. ***Recuperación y reanudación:*** esta etapa tiene que ver con las actividades de las siguientes instalaciones; sitio original dañado, sitio alterno de TI de recuperación, área de oficinas alternas, sitio alterno para la prestación del servicio.
6. ***Normalización:*** en este periodo final se debe considerar todos los cambios que ya han sido aplicados para retornar al sitio original o bien a un sitio nuevo. Para ello también se propone tener en cuenta la *Norma ISO 22316 de 2018* que habla de todo lo que es la resiliencia organizacional como “la capacidad que una organización tiene para absorber un ambiente cambiante y adaptarse a él, lo que le posibilita cumplir sus objetivos, sobrevivir y prosperar.

   Las organizaciones con mayor resiliencia pueden anticiparse y responder a las amenazas y oportunidades que surgen de cambios graduales o repentinos en su contexto interno y externo. La mejora de la resiliencia puede ser una meta organizacional estratégica”. (ICONTEC, 2018). Esto se lleva a cabo de manera posterior cuando se llegue a la etapa de retorno normal en la operación, donde debe de

generarse en el plan una articulación para adaptarse a los cambios, teniendo así la organización la capacidad o cualidad para recuperarse y retornar en un entorno diferente.

7.1.3. Plan de Recuperación de Procesos

Cada proceso debe contar con un procedimiento establecido para la recuperación del mismo, una vez haya ocurrido un incidente perjudicial, teniendo en cuenta asuntos necesarios para la reactivación como: insumos, personas asociadas, tiempo, lugar de ejecución y servicios a entregar. Este ayuda a regresar al estado previo a la contingencia que haya ocurrido en el momento, desplegando así su activación, luego de la actuación del OD-GH-03 Plan de prevención, atención y respuesta ante emergencias.

Este plan es la primera respuesta que se da una vez presentado el evento disruptivo, haciendo así un análisis del impacto según los escenarios que ya se tienen previstos, para cumplir con la ruta a seguir dentro del PCN y el Comité de Continuidad debe tener las bases para decidir si activar o no la estrategia del PCN. La estrategia define para la recuperación de procesos del PCN, incluye esos planes contingencia relacionada con las personas y las instalaciones para soportar la operación de los procesos críticos de la organización.

De allí la importancia del BIA como elemento fundamental para la recuperación, al saber cómo me impacta, puede documentar como actuar frente al evento y que necesito en cuanto a recursos físicos y tecnológicos, presupuesto y personal para responder la continuidad del proceso.

7.1.4. Plan de Recuperación Tecnológica (DRP)

El plan de continuidad en lo relacionado a este ítem debe desarrollar de tal forma que permita garantizar la restauración oportuna de las operaciones esenciales de la EPS, se acoge acá la sugerencia de MinTIC al respecto cuando expresa que la “implementación de un proceso de preservación de la información pública ante situaciones disruptivas permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación” (MinTIC, 2010)

La organización dado el rediseño que está efectuando actualmente del Data center, debe ampararse en la creación del DRP; considerando que es el nuevo aplicativo misional conocido como *Somos +*, la implementación de procedimientos para acceder a los sistemas de información críticos identificados en el BIA tecnológico, dado que encontraron un nivel de vulnerabilidad alto del acceso al aplicativo, falta de políticas de seguridad del sistema y la información debidamente socializadas, no definición clara de procesos (procedimiento modificación de usuarios) y no existía la claridad en algunos procedimientos de seguridad de la información.

Ahora con la claridad de los soportes desde primer nivel que se realiza por medio del "Procedimiento tecnológico de mesa de ayuda" hasta llegar a la activación del DRP; el plan de continuidad y el plan de recuperación son respaldos, ante una falla que inhabilite de manera parcial o total alguno de los servidores de cualquiera de los centros de datos, los cuales están involucrados en la prestación directa o indirecta de los servicios de afiliados de la EPS o servicios internos. Teniendo así definido el tiempo interrupción tolerable para cada componente de su soporte técnico, definidos de la siguiente manera:

Componente	Descripción	Tiempo de interrupción tolerable (RTO)
Aplicaciones	Somos+ (App)	90 minutos (mes)
	Base de datos somos+	90 minutos (mes)
Infraestructura	Máquinas virtuales (V.M.)	90 minutos (mes)
Comunicaciones	Enlaces con Internet Enlaces MPLS	90 minutos (mes)

Tabla 20 Tiempo de interrupción tolerable DRP
Fuente: Plan de Recuperación de Desastre en construcción de Savia Salud EPS

Si estos escenarios no estuvieran contemplados no podrían realizarse afiliaciones y autorizaciones, se tendría perdida de información, colapso del sistema, limitación de almacenamiento, entre otros. Desde el OD-TI-07 Plan estratégico de tecnologías de la información y comunicación logrando así restablecer la disponibilidad de estos, con las condiciones de Seguridad de la Información establecidas para la operación, contando así con toda una estructura de contingencia con un segundo cuarto de datos.

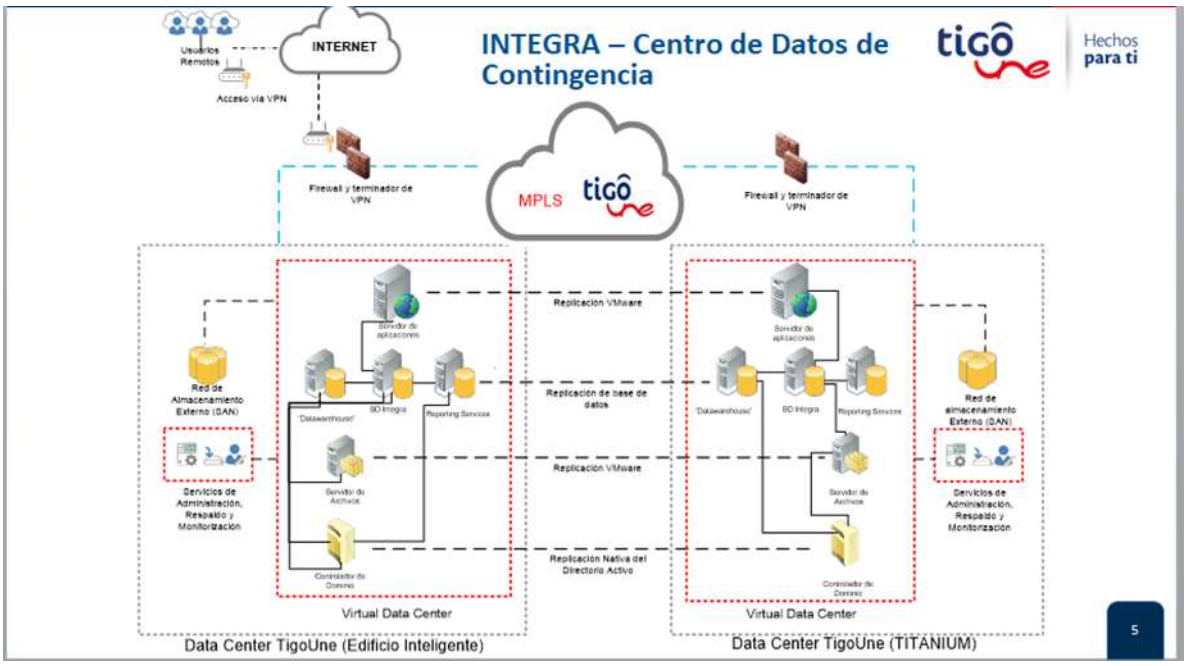


Tabla 21 Descripción del esquema de contingencia en un segundo centro de datos
Fuente: Plan estratégico de tecnologías de la información y comunicación de Savia Salud EPS

Las acciones de contingencia son soportes tecnológicos que cada proceso de la dependencia debe crear y articularlas a las necesidades del proceso misional, en primera instancia, así representa y garantiza las copias de seguridad en cuando a: bases de datos, servicios de aplicativos, información en red y computadores, entre otros, que garanticen continuar la operación sin incidentes que afecte la totalidad del Data Center principal. Para ellos todos estos soportes y los demás que sean necesarios según las necesidades identificadas deben estar en el centro alterno de datos, contando Savia Salud EPS con uno en Medellín y otro en Bogotá.

Tomar las siguientes acciones preventivas son necesarias a implementar por la dependencia de Tecnologia e Información para asegurar el servicio:

- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con canales de comunicación alternativo.
- Contar con mantenimiento preventivo para dichos equipos.
- Contar con los Backup de información necesaria para restablecer las aplicaciones.
- Contar con Backup de las aplicaciones y de las bases de datos.
- Almacenar en un lugar seguro los Backup referidos a aplicaciones y datos. Se recomienda el almacenamiento de los Backup en un lugar externo fuera de las instalaciones.

7.1.5. Retorno de la Operación con normalidad

Savia Salud EPS, debe retornar a la operación normal de sus sistemas de información y proceso misional, una vez sea expresado por el Comité de Continuidad, en apoyo del comité de emergencias para tomar la decisión de desactivar el PCN, pasado y logrado sobreponerse ante el evento disruptivo. Esta decisión se comunica mediante la dependencia de Comunicaciones Corporativas (líder de comunicaciones) para usar el protocolo de Comunicación en Crisis, el cual debe estar actualizado para utilizar los protocolos respectivos, tanto a nivel interno y con los diferentes grupos de interés para reanudar la operación con normalidad.

La dependencia de Planeación y Gestión del Conocimiento (Líder de Planeación), utiliza el protocolo de comunicaciones con la dependencia de Comunicaciones Corporativas, para informar la restauración de las actividades, generando consigo informe de evaluación y si la restauración no trajo consigo elementos que no se tenían absueltos, para así, realizar planes de mejora e incorporar lo no previsto dentro del PCN, como también se tendrá que divulgar de manera externa el normal funcionamiento de la operación.

La estrategia de Continuidad del negocio se dirige en promover la resiliencia organizacional entre los empleados, con el desarrollando de actividades que le permitan a la EPS tener la capacidad de recuperarse tras la ocurrencia de un evento disruptivo, recuperando la operación en situaciones alterables que cambian la dinámica de la organización.

9. EJERCICIOS Y PRUEBAS

Para saber que tan efectivo el plan puede ser durante la contingencia es necesario garantizar ejercicios y descripción de pruebas, que se puedan realizar como simulacros, medición de asignación de recursos, tiempos estimados, personal adecuado, efectiva socialización y conocimiento por parte de los empleados, entre otras. Son acciones que permiten disminuir el error, saber cuál es la capacidad y cómo es la oportunidad de reacción ante el evento.

Para ellos una vez al año se debe fijar un objetivo de prueba, que permita generar un alcance para saber qué proceso puede entrar en simulación de afectación, determinar el personal involucrado, medios disponibles para operar, fechas y horas de programación para el ejercicio, y revisar los resultados con relación a los escenarios planteados. Teniendo en cuenta que se debe generar un presupuesto por parte del Comité de Continuidad para cada uno de los simulacros, algunas acciones que se pueden beneficiar y dar un resultado del desarrollo del PCN son:

- Simulacro de evacuación: ejercicio y prueba de la efectividad del plan de evacuación.
- Práctica de confirmación de bienestar: realiza las llamadas a los empleados.
- Práctica de lanzamiento del Comité de Continuidad: llamada a cada miembro y que cada uno conduzca su rol.
- Recuperación de datos: ejercicios y prueba tu sistema de resguardo de datos TI.
- Reiniciar operaciones: realizar el reinicio de actividades de los procesos críticos como, no tener sistema, red o energía.
- Operar sitio alterno: ejercicios y pruebas del lugar alternativo de operaciones para algún proceso.

El resultado de estos se puede medir mediante indicadores, auditorias u otras herramientas que pueden arrojar una mejor planeación a cargo de los responsables, mediante acciones correctivas y preventivas, saber el nivel de madurez con el que puede ejercer el plan y conllevar así a realizar planes de mejora, para asegurar el mayor porcentaje de error ante un escenario real de desastre. Para esto se sugiere tener en cuenta los siguientes indicadores que dan resultados cualitativos y cuantitativos para saber la efectividad del PCN.

KPI (key performance indicator): siendo una herramienta cualitativa en la cual se realiza un juego de indicadores, donde “la selección de indicadores clave de rendimiento es una decisión importante que puede tener muchas implicaciones potenciales”. (Márquez & Crespo Márquez, 2012, pág. 25) Para medir el desempeño de las actividades desarrolladas en la continuidad del negocio, al tener un despliegue de estructura de procesos críticos según el tipo de riesgo al que se encuentre expuesto, los siguientes son algunos indicadores que pueden permitir la medición de la efectividad de las actividades designadas en el PCN:

INDICADOR: Nivel de Impacto	
Objetivo del indicador:	**Fórmula**
Definir el % de riesgo ocurrido frente a lo asumido por los procesos críticos en su prevención del riesgo.	$\text{Nivel de Impacto} = \frac{\text{Impacto del riesgo}}{\text{Total de impacto del riesgo asumido}}$
INDICADOR: Oportunidad en el plan de continuidad	
Objetivo del indicador:	**Fórmula**
Cumplir con el tiempo de reacción en la activación del plan según lo estipulado.	$\text{Oportunidad en el plan de continuidad} = \frac{\text{Oportunidad de reacción}}{\text{Tiempo pronosticado para el proceso}}$
INDICADOR: Efectividad en la asignación de recursos	
Objetivo del indicador:	**Fórmula**
Utilizar los recursos necesarios para que el PCN sea efectivo a la hora de entrar en curso frente a un evento disruptivo.	$\text{Efectividad en la asignación de recursos} = \frac{\text{Recursos utilizados}}{\text{Total de recursos asignados}}$

Tabla 22 Indicadores de desempeño de actividades
Fuente: Elaboración propia para medición cualitativa de actividades del PCN

Desde lo cuantitativo se debe contar con indicadores que soporten el negocio para retornar a la normal operación, siendo los siguientes una posible medición para demostrar el impacto del PCN:

INDICADOR: Retorno de actividades	
Objetivo del indicador:	**Fórmula**
Retomar la operación con las acciones estipuladas para normalizar los procesos afectados.	$\text{Retorno de actividades} = \frac{\text{Retorno a la normalidad}}{\text{Total asignado como normal operacional}}$
INDICADOR: Plan de formación	
Objetivo del indicador:	**Fórmula**
% de cumplimiento en capacitación a todos los involucrados para tener claridad de sus roles y responsabilidades a la hora de un evento disruptivo.	$\text{Plan de formación} = \frac{\text{Capacitación de PCN}}{\text{Total capacitaciones estipuladas}}$
INDICADOR: Nivel de Auditorías	
Objetivo del indicador:	**Fórmula**
% de cumplimiento de control y seguimiento en prevenir e identificar nuevas acciones a proteger en un evento disruptivo.	$\text{Nivel de auditorías} = \frac{\text{\# de auditorías de intervención PCN}}{\text{Total de auditorías programadas}}$
INDICADOR: Evaluación de procesos	
Objetivo del indicador:	**Fórmula**
Tener el mayor % de procesos críticos protegidos e identificados para una mayor eficiencia en la seguridad de los servicios.	$\text{Evaluación de procesos} = \frac{\text{\# de procesos críticos evaluados}}{\text{Total de procesos críticos documentados}}$
INDICADOR: Planes de contingencia	
Objetivo del indicador:	**Fórmula**
Crear los planes de contingencia necesarios para prevenir y mitigar los impactos que puedan ocasionar un evento disruptivo.	$\text{Planes de contingencia} = \frac{\text{Planes contingencia formulados}}{\text{Total de planes de contingencia planeados}}$

Tabla 23 Indicadores de desempeño de actividades
Fuente: Elaboración propia para medición cualitativa de actividades del PCN

El resultado de estos ejercicio y pruebas se dan de acuerdo a como cada uno de ellos se encuentre desarrollado, generando así con anterioridad del simulacro anual los responsables, los participantes en la ejecución, el paso a paso de los procedimientos; según el riesgo que ya se encuentran documentados, y la generación de informes de los ejercicio y pruebas para la toma de decisiones que identifiquen oportunidades de mejora.

10. MEJORA CONTINUA

Los informes realizados en la etapa de ejercicios y pruebas identifican oportunidades de mejora, creando un registro de lecciones aprendidas y teniendo elementos para identificar los puntos de falla del PCN. Cuando se habla de un plan de mejora es importante recrear un inicio de acciones mediante la herramienta del ciclo PHVA, donde se hará un diagnóstico de lo sucedido, se hará una evaluación del proceso según los resultados en cuanto a la optimización de recursos, protocolos, procedimientos y planes en cuestión durante el simulacro realizado.

Así mismo, la mejora continua permite ampliar la capacidad de respuesta ante el evento, llevando así a modificar medidas, estrategias, actualizar o crear nuevos procedimientos o planes que aumente el nivel de madurez del PCN. Para ello, se tiene en consideración la realización del Modelo de Gestión de Nivel de Madurez, la cual sirve como herramienta de evaluación del sistema de gestión que tiene un plan, así se puede determinar mediante la creación de criterios, los cuales se realizaron con base en la Resolución 1445 de 2006 Sistema Único de Acreditación - SUA para EAPB.

Los elementos clave para la evaluación están divididos en los siguientes cuatro elementos de la Gestión del Riesgo, conocidos como: Gobierno, Proceso, Personas y Tecnología; estos cuentan con un total de 34 criterios los cuales se realizaron desde la dependencia de planeación y Gestión del conocimiento para dar una calificación individual a cada criterio y así mismo saber en qué nivel de madurez de la gestión se encuentra el PCN.

Los criterios para definir la calificación de cada uno de los elementos, se hace mediante las siguientes tres dimensiones: enfoque, implementación y resultados. A continuación se plasma la definición de cada dimensión, las variables y su respectiva descripción.

- **Enfoque**. Se refiere a las directrices, métodos y procesos que la institución utiliza para ejecutar y lograr el propósito solicitado en cada tema o variable que se va a evaluar.

Variables:

Sistematicidad: Grado en que el enfoque es definido y aplicado de manera organizada.

Amplitud: grado en que el enfoque está presente y orienta las diferentes áreas de la organización o distintos puntos del capítulo.
Proactividad: grado en que el enfoque es preventivo y proactivo.
Ciclo de Evaluación y mejoramiento: forma en que se evalúa y mejora el enfoque
Impacto: grado de incidencia del enfoque en la implementación y en los resultados.

- **Implementación.** Se refiere a la aplicación del enfoque, a su alcance y extensión dentro de la institución.

Variables:
Despliegue de la institución: grado en que se ha implementado el enfoque y es consistente en las distintas áreas de la organización o los distintos puntos del capítulo.
Despliegue hacia el cliente: grado en que se ha implementado el enfoque y es percibido por los clientes internos y/o externos, según la naturaleza y propósitos del estándar.

- **Resultados.** Se refiere a los logros y efectos de la aplicación de los enfoques.

Variables:
Pertinencia: es el grado en el cual los usuarios obtienen los servicios que requieren, con la mejor utilización de los recursos de acuerdo con la evidencia científica y sus efectos secundarios son menores que los beneficios potenciales.
Avance de la medición: grado de ejecución e implementación del sistema.
Comparación: observar las diferencias y las semejanzas entre dos elementos, sean personas, procesos, actividades, entre otros.

El nivel de madurez en la gestión de riesgos ayuda a “determinar el nivel de desarrollo de la gestión de riesgos es clave para poder avanzar en su mejora como elemento fundamental de protección, sostenibilidad, buen gobierno corporativo y crecimiento, integrando dicha gestión en la planeación estratégica de la compañía”. (RIMS, 2018) Para saber este rendimiento se establece una calificación desarrolladas en cinco niveles compuestos de la siguiente manera:

Nivel 1. No desarrollado: no existe un enfoque estructurado para identificar y gestionar los riesgos. Las prácticas de gestión de riesgos son básicas y no son aplicadas de manera

consistente, y existe un bajo nivel de entendimiento y conciencia sobre las mismas. Hay oportunidades de mejora críticas.

Nivel 2. Formalizado: políticas y procesos están siendo establecidos. Las prácticas de gestión de riesgos están en proceso de desarrollo, no son aplicadas de manera consistente, pero existe un buen entendimiento y conciencia sobre las mismas por unos pocos individuos en la organización. Hay oportunidades de mejora significativas.

Nivel 3. Establecido: la gestión de riesgos ha sido implementada dentro de los procesos rutinarios de la organización. Las prácticas de gestión de riesgos están establecidas, se aplican de manera consistente con mejores niveles de entendimiento y conciencia sobre las mismas por la gerencia y por los empleados. Hay oportunidades de mejora en ciertos aspectos.

Nivel 4. Implantado e interiorizado: existe un enfoque proactivo frente a la gestión de riesgos en todos los niveles de la organización. Las prácticas de gestión de riesgos están en un nivel avanzado, se aplican de manera consistente y están incorporadas en los procesos con altos niveles de entendimiento y conciencia por parte de la gerencia y los empleados. Hay oportunidades de mejora en unos pocos aspectos puntuales.

Nivel 5. Optimizado: se está llevando a cabo mejora continua y la gama completa de actividades del programa de gestión de riesgos se están ejecutando. Las prácticas de gestión de riesgos son innovadoras y vanguardistas en la industria, se aplican de manera consistente, están integradas transversalmente en la organización y son fácilmente replicables en nuevas áreas de la organización. Hay muy altos niveles de entendimiento y conciencia sobre las prácticas de gestión de riesgos por parte de la gerencia y los empleados.

A continuación, en la tabla 22 se ilustra la calificación que se le daría a cada uno de los criterios, el cual tendrá una ponderación según su nivel de madurez.

N° niveles	Nivel de madurez de la gestión	Calificación indivudual por criterio	Calificación Ponderada
Nivel1	No desarrollado	3-5	
Nivel2	Formalizado	6- 8	
Nivel3	Establecido	9 - 11	
Nivel4	Implantado e interiorizado	12 - 13	
Nivel 5	Optimizado	14-15	

Tabla 24 Calificación Nivel de Madurez de Gestión para PCN
Fuente: Elaboración propia con dependencia de Planeación y Gestión del Conocimiento

La herramienta se anexa en formato Excel "Herramienta de Medición de la Gestión de Nivel de Madurez", la cual sirve como método de calificación de madurez para el PCN, con el propósito de desarrollar y analizar el nivel de avance buscando así la mejora continua en la continuidad de la operación, mejorar en los procesos de planificación, de análisis y gestión de los riesgos a los que puede estar expuesto la organización.

REFERENTE BIBLIOGRÁFICO

APEC. (2014). *APEC MSME MARKET PLACE*. Obtenido de APEC MSME MARKET PLACE: https://apecmsmemarketplace.com/sites/default/files/doc/bcp_guidebook_abridged_version_spanish_20140829.pdf

Business Continuity Institute. (s.f.). Obtenido de https://www.thebci.org/

Departamento Nacional de Planeación - DNP. (s.f.). Obtenido de DNP: https://www.dnp.gov.co/programas/desarrollo-social/subdireccion-de-salud/Paginas/aseguramiento.aspx

Departamento Nacional de Planeación - DNP. (11 de Noviembre de 2016). Obtenido de DNP: https://www.dnp.gov.co/programas/desarrollo-social/subdireccion-de-salud/Paginas/aseguramiento.aspx

Disaster Recovery Institute International. (s.f.). Obtenido de https://drii.org/

ICONTEC. (s.f.). Obtenido de www.icontec.org

ICONTEC. (2012). *Norma ISO 22301*. Obtenido de https://kupdf.net/download/norma-iso-22301-castellano_5b6c10a9e2b6f52555f6a894_pdf

ICONTEC. (2012). Norma ISO 22301.

ICONTEC. (2018). *NORMA ISO 22316*. Obtenido de https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO22316.pdf

Márquez, C. A., & Crespo Márquez, A. (2012). *Ingeniería de Mantenimiento y Fiabilidad Aplicada en la Gestión d eActivos.* Sevilla: INGEMA.

MinTIC. (2010). *Guía para la preparación de las TIC para la continuidad del negocio.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

National Institute of Standards and Technology. (s.f.).

RIMS. (2018). *Navegando la incertidumbre - III BENCHMARK DE GESTIÓN DE RIESGOS EN LATINOAMÉRICA.* Nueva York, NY.

Unipiloto. (11 de Septiembre de 2001). *Universidad Piloto de Colombia.* Obtenido de http://polux.unipiloto.edu.co:8080/00001889.pdf