TABLA DE CONTENIDO

1 INTRODUCCIÓN 3

2 ALCANCE 3

3 DEFINICIONES 3

4 OBJETIVOS 8

5 PRINCIPIOS DE LA POLÍTICA CORPORATIVA DE CONTINUIDAD DE NEGOCIO 9

6 ROLES Y RESPONSABILIDADES DEL SGCN 11

7 ESTÁNDARES DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO (SGCN) 14

7.1 ANÁLISIS DE IMPACTO DE NEGOCIO (BIA). 14

7.2 ANÁLISIS DE RIESGOS 15

7.3 ESTRATEGIAS DE CONTINUIDAD 15

7.4 DESARROLLO DEL PLAN DE CONTINUIDAD DE NEGOCIO (PCN). 17

7.4.1 Procedimientos de gestión de crisis 17

7.4.2 Planes de recuperación de negocio 17

7.4.3 Organización del SGCN 17

7.4.4 Protocolo de Comunicación 17

7.4.5 Plan de Formación 18

7.4.6 Plan de Pruebas 18

7.5 PROCEDIMIENTO DE MANTENIMIENTO DEL PCN 19

7.6 SEGUIMIENTO Y MEJORA CONTINUA DEL SGCN 19

8 DOCUMENTOS DE REFERENCIA 19

9 CONTROL DE CAMBIOS 19

10 FIRMAS DE REVISIÓN Y APROBACIÓN 20

1 INTRODUCCIÓN

El Sistema de Gestión de Continuidad de Negocio (SGCN) es un proceso de gestión holístico que identifica los impactos potenciales que amenazan a **PROINDESA S.A.S Y SUS SOCIEDADES ADMINISTRADAS**[1]**,** en adelante **"la Organización",** y que proporciona un marco de actuación para garantizar su resiliencia y la capacidad de una respuesta efectiva, que permita minimizar el impacto de una eventual interrupción de la operativa de negocio, proteger la reputación, la imagen de marca y salvaguardar los intereses de sus principales partes interesadas.

2 ALCANCE

El presente documento establece la Política de Continuidad de Negocio de **LA ORGANIZACIÓN**, que se aplicará para el desarrollo e implementación del Sistema de Gestión de Continuidad de Negocio (SGCN) de Proindesa y sus sociedades administradas.

3 DEFINICIONES

- **Actividad o Proceso Crítico:** Actividades o procesos que se llevan a cabo para desarrollar los productos y servicios clave que permiten a la Organización alcanzar sus objetivos más importantes. Incluye las actividades de soporte imprescindibles.

- **Actividad o Proceso No Crítico:** Actividades o procesos cuya interrupción puede ser asumida temporalmente por la Organización.

- **Acuerdo de nivel de servicio (ANS):** Es un acuerdo escrito entre el proveedor de servicio (interno o externo) y su cliente, que contiene la naturaleza, calidad, disponibilidad, alcance y respuesta del proveedor de servicio, y las responsabilidades de ambos.

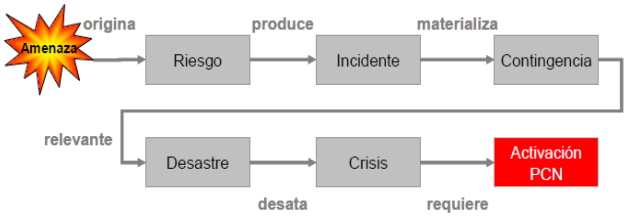
- **Activos soporte:** se compone de la información, recurso humano, equipos e instalaciones de la Organización.
- **Administración:** Presidente, Vicepresidentes de la Organización y quienes hagan sus veces en las sociedades administradas.

- **Alta Dirección**, Junta Directiva, Presidente, Representantes Legales, Vicepresidentes de la Organización y quienes hagan sus veces en sus sociedades administradas.

[1] Corresponde a aquellas compañías con las cuales Proindesa SAS tiene vigente un Acuerdo de Colaboración Empresarial.

- **Alerta:** Notificación formal de que ha ocurrido un incidente o contingencia que puede dar lugar a la puesta en marcha del Plan de Continuidad.

- **Amenaza:** hecho que puede producir un daño. Es la causa potencial de un daño a un activo. Un evento o incidente provocado por una entidad natural, humana o artificial que, aprovechando una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de ese activo.



- **Análisis de riesgos:** Proceso sistemático que permite estimar la magnitud de los riesgos a los que se encuentra expuesta la Organización, mediante la identificación de las amenazas y vulnerabilidades asociadas los distintos activos que la integran y la estimación del impacto y la probabilidad de materialización de estas amenazas.

- **BIA (Business Impact Analysis - Análisis de impacto del negocio):** Informe que muestra el costo ocasionado por la interrupción de los procesos de negocio. Una vez se obtiene este informe, la Organización tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante, establecer la prioridad de recuperación (o su orden secuencial).

- **BCP (Business Continuity Planning – Plan de Continuidad del Negocio):** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro, abarca tanto la Planeación para Recuperación de Desastres (DRP) como la Planeación para el Restablecimiento del Negocio. Ambos se diferencian de la Planeación de Prevención de Pérdidas, la cual implica la calendarización de actividades como respaldo de sistemas, autenticación y autorización (seguridad), revisión de virus y monitoreo de la utilización de sistemas (principalmente para verificaciones de capacidad).

- **(CAP) Centro Alterno de Procesamiento:** el sitio alterno donde estarán los servicios tecnológicos de la empresa en contingencia.

- **Ciclo de Gestión de la Continuidad de Negocio**: Serie de actividades y procesos que son necesarios para gestionar la continuidad de negocio. Consta al menos de los siguientes elementos fases:
  - Conocimiento del negocio
  - Definición de la estrategia de continuidad
  - Desarrollo de un plan de continuidad
  - Formación
  - Pruebas y mantenimiento

- **Contingencia:** Materialización de un riesgo; evento que afecta a los procesos y/o activos de la organización y degrada o impide sus servicios hasta un punto donde el impacto financiero y/u operacional se convierte en inaceptable. Las contingencias pueden clasificarse en función del impacto que provocan, distinguiéndose las graves y las leves según activen o no el Plan de Continuidad de Negocio.

- **Control:** Medida técnica u organizativa que ayuda a mitigar el riesgo. Aplica a las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Crisis:** Situación anormal que amenaza las operaciones, la plantilla, los clientes y/o la reputación de una empresa. Una contingencia lleva aparejada la situación de crisis en la Organización

- **Desastre:** Materialización de una contingencia relevante (anticipada o inesperada), que imposibilita total o parcialmente el mantenimiento de las funciones críticas de negocio durante un periodo de predeterminado tiempo.

- **DRP (Disaster Recovery Planning - Plan de Recuperación de Desastres):** Conjunto de procedimientos y actividades de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave.

- **Escenario**: Situación definida a priori, a la que se llegaría por uno o varios incidentes o contingencias, para hacer frente a la cual se preparan los planes de continuidad.

- **Estrategia de Continuidad de Negocio**: Enfoque adoptado por la Organización que determina los principios y objetivos de la continuidad de negocio ante una contingencia, en base a los cuales se elabora el Plan de Continuidad de Negocio.

- **Evacuación:** Movimiento de colaboradores, visitantes y proveedores de un centro a un lugar seguro de manera organizada tras la ocurrencia de un incidente o contingencia.

- **Gestión de Crisis**: Proceso en el cual la Organización gestiona el impacto de un evento o contingencia hasta que se encuentra controlado y sin impacto para ésta, o se invoca el Plan de Continuidad de Negocio como parte del proceso de Gestión de la Crisis.

- **Gestión de Continuidad de Negocio (BCM):** Proceso de gestión integral que identifica los impactos potenciales que amenazan una Organización y proporciona el marco de actuación para hacerla resistente, dotándola de capacidad de respuesta eficaz que salvaguarde los intereses de sus personas, la reputación, la imagen del nombre, la capacidad financiera y las actividades de creación de valor.

  También incluye la gestión del programa de formación, mantenimiento, revisión y realización de pruebas para mantener el Plan actualizado.

- **Impacto:** El costo para la Organización de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: ej., pérdida de reputación, implicaciones legales, etc.

- **MTPD (Maximum Tolerable Period of Disruption -Tiempo máximo de falla):** Tiempo Máximo de recuperación establecido después de la interrupción del servicio y la reanudación de este.

- **Tiempo de Recuperación Objetivo (RTO, Recovery Time Objective):** Periodo de tiempo durante el cual se puede suspender una tarea de negocio, producto o servicio, sistema o aplicación después de una contingencia, antes de que ocasione un impacto inaceptable para la Organización.

- **Persona Alternativa:** Aquella que sustituye a una persona crítica durante una crisis.

- **Personal de Continuidad:** Son todas aquellas personas que tienen alguna responsabilidad en los Comités y equipos de recuperación implicados en el Plan de Continuidad de Negocio.

- **Personal Crítico:** Personas encargadas de alguna actividad crítica dentro del Plan de Continuidad de Negocio, que deben conocerlo y, en caso de contingencia, llevar a cabo los Planes de Acción previamente definidos.

- **Procedimiento de Recuperación:** Conjunto de actividades a realizar para dar continuidad con la prestación del servicio en el momento de la interrupción o falla.

- **Procedimiento de Restauración:** Conjunto de actividades a realizar para volver a la normalidad.

- **Riesgo:** La probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro, éstas en conjunto se convierten en un riesgo.

- **RPO (Recovery Point Objective - Punto de Recuperación Objetivo):** Máximo periodo tolerable en el cual se puede presentar pérdida de datos o caída de la operación podrían perder sin afectar la operación.

- **RTO (Recovery Time Objective - Tiempo Objetivo de Recuperación):** Tiempo de referencia establecido para que los sistemas críticos de la operación estén nuevamente operando.

- **SARO (Sistema de Administración de Riesgo Operativo):** Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan, monitorean y mitigan el riesgo operacional.

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de toda la información sensible, electrónica o en otro formato, que es propiedad de la Organización.

- **Servicios Críticos:** Son aquellos servicios vitales para la operación de la Organización, y cuya interrupción representa serios riesgos de pérdida económica, operacional y/o de imagen; y pone en riesgo la viabilidad de la misma.

- **MBCO (Minimum Business Continuity Objective - Objetivo de Continuidad de Negocio Mínimo):** Es el nivel mínimo de servicios / productos aceptables que se debe garantizar en la Organización, tras una interrupción. Este dato es definido y aprobado por la Administración

- **Vulnerabilidad:** Carencia o debilidad de control asociada a un activo, que puede facilitar la materialización de una amenaza que se cierne sobre dicho activo.

4 OBJETIVOS

La implementación de un sistema de gestión de continuidad de negocio persigue como objetivos principales:

- Salvaguardar la integridad del personal en una situación de contingencia.
- Mantener la liquidez de la Organización.
- Minimizar las pérdidas económicas para la Organización.
- Establecer procedimientos de recuperación de la operativa de negocio eficaces y eficientes en caso de contingencia.
- Garantizar la estabilidad del (os) Sistema(s) utilizado(s) en la Organización.
- Cumplimiento de los requerimientos regulatorios.
- Mantener la imagen del nombre de la Organización.
- Mantener la confianza de clientes y principales partes interesadas.

En lo relativo al alcance del SGCN la Organización debe:

- Asegurar que se encuentren claramente establecidas las responsabilidades para la gestión de la continuidad de negocio.
- Garantizar que se asignan los recursos necesarios para establecer y mantener el SGCN.

- Definir los servicios y/o procesos que deben incluirse en el ámbito de aplicación del sistema de gestión.
- Identificar las dependencias de estos servicios y/o procesos, incluyendo proveedores de suministros y servicios externalizados y otras terceras partes relevantes.
- Tener en cuenta los intereses, necesidades y expectativas de las terceras partes interesadas.
- Cumplir con los requerimientos legales y regulatorios.
- Aseguran que el alcance del SGCN es apropiado al tamaño, complejidad y naturaleza de la Organización y que considera en su definición, la misión y objetivos de esta.

5 PRINCIPIOS DE LA POLÍTICA CORPORATIVA DE CONTINUIDAD DE NEGOCIO

La Organización cumpliendo con las directrices marcadas en la presente política, desarrolla un sistema de gestión de continuidad de negocio (SGCN), de acuerdo con los siguientes principios:

- La Organización tiene que definir y mantener un (SGCN) que permita minimizar los riesgos de esta y el impacto sobre el servicio en caso de un evento de desastre o contingencia grave que cause la interrupción de la actividad de negocio.

- La Alta Dirección es la responsable de supervisar el desarrollo, la implantación y el mantenimiento del SGCN de la Organización.

- La Alta Dirección designa a un responsable (o equipo) para el desarrollo y mantenimiento del SGCN. Este responsable será quien presida y organice la gestión de continuidad de negocio de la Organización.

- Los dueños de proceso deben asignar responsables para coordinar la realización de análisis de impacto de negocio (BIA) y la definición de planes de recuperación para áreas de negocio. Estos responsables serán también los enlaces de las unidades durante la gestión de una crisis causada por un evento de desastre.

  Es importante señalar que, se considera que siempre que el responsable de un Proceso/Subproceso no se encuentre disponible, la responsabilidad recaerá sobre su superior inmediato.

- Las Direcciones de soporte (Dirección de Tecnología y Dirección Administrativa) deben asignar colaboradores para coordinar la definición de planes de contingencia que soporten a las áreas de negocio en la recuperación de los procesos críticos identificados en el BIA. Los planes y procedimientos incluidos el plan de recuperación de desastres (DRP) de la Dirección de Tecnología, tienen que estar alineados con los requerimientos identificados en el BIA por las áreas de negocio.

- Con base en los resultados del BIA, la Organización debe realizar un análisis de riesgos en el que se identifiquen los escenarios de contingencia que puedan impactar en la continuidad de los procesos críticos identificados. Las estrategias de continuidad tienen que ser definidas e implantadas para cada escenario de contingencia identificado.

- Como respuesta a los escenarios de contingencia identificados, se tienen que definir procedimientos de gestión de crisis que incluyan la designación de equipos para la gestión de estas, criterios de activación del plan de continuidad de negocio (PCN) y protocolos de comunicación interna y externa durante la crisis. De manera adicional, se tiene que establecer un procedimiento para informar al equipo de continuidad de negocio respecto a la activación del PCN de La Organización.

- La Organización debe diseñar un programa de formación que permita proporcionar la instrucción necesaria para los colaboradores involucrados en las actividades del plan de continuidad de negocio y que este contemple iniciativas de divulgación para concienciar a los todos los colaboradores sobre sus responsabilidades en la gestión de continuidad de negocio.

- La Organización debe establecer un plan de pruebas que permita verificar la validez y eficacia de los planes de recuperación de negocio y de los planes de recuperación de desastres Tecnología (TI). El plan de pruebas y las principales conclusiones de este debe presentarse a la Administración de la Organización de manera periódica.

- La Organización debe establecer procedimientos que garanticen el mantenimiento y la actualización de su SGCN, especificando responsabilidades y periodicidades. El SGCN y sus actualizaciones tiene que ser presentado y aprobado por la Junta Directa o quien haga sus veces en la Organización.

6 ROLES Y RESPONSABILIDADES DEL SGCN

La Dirección de Riesgos, es la responsable de recomendar la Política, los estándares y el modelo de referencia de Gestión de Continuidad de Negocio de la Organización.

A continuación, se describen los roles y responsabilidades para la definición y mantenimiento del SGCN de la Organización:

- La **Junta Directiva o quien haga sus veces** es el máximo responsable para la supervisión del desarrollo, implantación y mantenimiento del SGCN.

- La **Administración** tendrá como rol dentro de la continuidad de negocio, demostrando liderazgo y compromiso con el SGCN:

  - Asegurando que la política, los estándares y los objetivos de gestión de continuidad de negocio son establecidos y están alineados con los objetivos y la estrategia de negocio de la Organización.
  - Asignando los recursos necesarios para el desarrollo, la implantación y el mantenimiento del SGCN.
  - Designando al responsable para la implantación y mantenimiento del SGCN, el cual deberá contar con la apropiada autoridad y competencia.
  - Asegurando que el SGCN es actualizado al menos de manera anual.
  - Garantizando que los planes y procedimientos incluidos en el SGCN son ejercitados y probados de manera periódica (al menos anualmente) y revisando el plan de pruebas y los resultados de este de forma regular.
  - Asegurando que los colaboradores y las terceras partes interesadas son formados y conscientes sus responsabilidades respecto a la gestión de continuidad de negocio (en los casos que aplique)
  - Garantizando que se realizan auditorias periódicas del SGCN.
  - Promoviendo la mejora continua del SGCN.

- **Dirección de Riesgos:** Será responsable de garantizar que:
  - Se desarrollen y mantengan planes y procedimientos de continuidad de negocio, conformes a los definidos en la Política de Continuidad de Negocio de la Organización.
  - Los participantes en las actividades del SGCN reciban la formación y el entrenamiento adecuados.

- Se establezcan y documenten los procedimientos necesarios de comunicación y del escalamiento.
- Se ejecuten pruebas periódicas del PCN.
- De manera adicional, durante la crisis las responsabilidades de esta Dirección incluirán:
  - ✓ La evaluación conjunta con la Dirección de Tecnología, del impacto y la criticidad de los servicios y productos afectados por la contingencia.
  - ✓ La declaración de la contingencia y el reporte a la Administración.
  - ✓ La confirmación de la activación de los equipos de emergencia y recuperación correspondientes.
  - ✓ El reporte periódico a la Administración sobre la evolución de la contingencia y de las tareas de recuperación, en el caso de que el PCN haya sido activado.

- **Director de Riesgos o quien haga sus veces:** Persona designada por la Administración para:
  - Mantener la Política de continuidad de negocio de la Organización.
  - Dar soporte a las unidades de negocio en el análisis de impacto de negocio (BIA) y en la definición de sus planes de recuperación.
  - Apoyar a la Dirección de Tecnología y/o a la Dirección Administrativa en la definición de sus planes de contingencia.
  - Coordinar y ejecutar el plan de pruebas de la Organización**.**
  - Monitorear los cambios normativos o regulatorios que puedan afectar a la gestión de continuidad de negocio de la Organización.

- **Directores y/o Gerentes de las áreas de Negocio.**
  Deben asegurar el compromiso y el cumplimiento de todos los colaboradores que componen sus áreas con la política de continuidad de negocio. Serán responsables de designar a uno o varios colaboradores que se encarguen de gestionar el desarrollo y el mantenimiento de los planes de continuidad/recuperación de negocio para sus respectivas áreas.

- **Áreas de Soporte[2].**
  Serán las responsables de desarrollar y establecer planes de contingencia que garanticen la disponibilidad de las actividades de soporte necesarias para la recuperación de los procesos críticos de negocio, en los tiempos requeridos.

[2] Incluye a la Dirección de Riesgos con su área de seguridad de la información

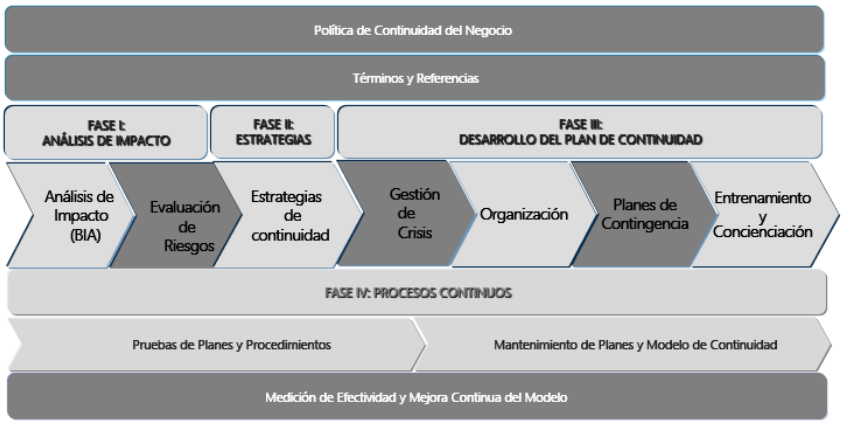
- **Dirección Administrativa:**
  - ✓ Definir los procedimientos de emergencia y evacuación que garanticen la integridad física de los colaboradores en el caso de una contingencia grave en las instalaciones.
  - ✓ Establecer procedimientos de comunicación interna con colaboradores durante la crisis.
  - ✓ Coordinar los protocolos de atención primaria (primeros auxilios) y la comunicación con familiares en el caso de que haya colaboradores heridos o fallecidos como consecuencia de la contingencia.
  - ✓ Establecer y coordinar procedimientos de contratación de emergencia en caso de que sea necesario reforzar alguna actividad crítica durante la contingencia.
  - ✓ Definir procedimientos de emergencia y evacuación, de acuerdo con la legislación vigente de forma que se garantice la integridad física de los colaboradores de la Organización.
  - ✓ Designar espacios alternativos para la recuperación de los procesos críticos tan pronto como sea posible.
  - ✓ Proporcionar salas específicas y equipadas para la gestión de crisis.
  - ✓ Establecer los procedimientos logísticos para reubicar al personal crítico y al equipamiento requerido en las ubicaciones alternativas.
  - ✓ Garantizar la disponibilidad de los suministros clave (electricidad, agua, aire acondicionado, catering, etc.) en las ubicaciones de trabajo habituales y en las salas de contingencia designadas.

- **Dirección de Tecnología:**
  - ✓ Coordinar el desarrollo, prueba y mantenimiento de los planes de recuperación de desastres tecnológicos, asegurando su alineamiento con los requisitos de negocio identificados en el BIA.
  - ✓ Garantizar la disponibilidad de los sistemas, las comunicaciones y el equipamiento necesario en las ubicaciones alternativas, en base a los requerimientos establecidos en el BIA.

- **Auditoría Interna:** Serán los responsables de realizar revisiones periódicas independientes del SGCN.

7 ESTÁNDARES DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO (SGCN)

Como referencia a la hora de desarrollar el sistema de gestión de continuidad de negocio, la Organización toma como referencia la metodología descrita en el estándar internacional ISO 22301 en la que describe las fases y directrices generales del proyecto.



El SGCN de la Organización debe surtir las siguientes fases:

7.1 ANÁLISIS DE IMPACTO DE NEGOCIO (BIA).

En un BIA se analizan los procesos de negocio de la Organización para conocer qué impacto se produce en caso de que ocurra un incidente que cause la interrupción de estos procesos. Su objetivo es identificar cuáles son los procesos más críticos para la Organización.

La continuidad de negocio se debe centrar en aquellos procesos en los que la disponibilidad es vital, es decir, en caso de ser interrumpidos, el impacto que se ocasiona para la Organización puede ser no asumible en un espacio corto de tiempo.

El BIA debe contemplar los siguientes aspectos:

- **Identificar y priorizar los procesos y servicios críticos**: La priorización debe basarse en la severidad de las interrupciones potenciales de la actividad de negocio, determinada por su impacto financiero, operacional, legal y reputacional.

- **Determinar y documentar los requerimientos y recursos necesarios para recuperación de los procesos críticos identificados**: Personas necesarias para recuperar el proceso,

proveedores críticos, documentación vital, sistemas, comunicaciones y cualquier otro requerimiento tecnológico.

- **Estimación de los periodos máximos de interrupción, los tiempos de recuperación objetivo (RTO) y los puntos de recuperación de datos objetivo (RPO):**
  - ✓ Establecimiento de los niveles mínimos de servicio aceptables a los que se debe recuperar el proceso tras la interrupción.
  - ✓ Procedimientos manuales que describan las tareas a realizar en el caso de indisponibilidad de los sistemas que soportan el proceso.
  - ✓ Identificación de las posibles interdependencias entre procesos de negocio.
  - ✓ Determinación de la frecuencia y periodos críticos de ejecución para cada proceso.

Los resultados del BIA deben revisarse y aprobarse por los responsables de cada área de negocio y la Dirección de Riesgos, para posteriormente someter a aprobación de la Administración.

7.2 ANÁLISIS DE RIESGOS

Se identifican los escenarios de contingencia que pueden causar la interrupción de los procesos de negocio. Al menos, los siguientes tipos de escenarios de contingencia deben ser considerados:

- Impacto en edificios
- Impacto en sistemas de información.
- Impacto en personas.
- Impacto en proveedores críticos.

Para cada escenario, se deben determinar las amenazas o situaciones de riesgo que puedan causar la interrupción de la actividad de negocio, realizando una estimación de impacto y probabilidad.

7.3 ESTRATEGIAS DE CONTINUIDAD

Como respuesta a los escenarios de riesgos identificados, con base a los resultados del BIA y del análisis de riesgos, se definan e implementan las estrategias de continuidad.

Si se identifican varias y posibles estrategias para el mismo escenario, se realizará un análisis de costo-eficiencia en el que se sopesarán las posibles sinergias y el riesgo residual resultante

de la implantación de las distintas estrategias. De igual modo, si dos estrategias son complementarias para el mismo escenario y se implementan ambas, se indicará bajo qué situaciones se activará una u otra.

Las estrategias seleccionadas se deben presentar y aprobar por la Administración. Los siguientes aspectos deben ser considerados en la definición de las estrategias de continuidad:

- **Escenarios con impacto en edificios**: Espacio físico para alojar las salas de contingencia; número y tipo de puestos de trabajo alternativo (ordenadores portátiles, virtualización, etc.); impresoras, teléfonos fijos y celulares y otros elementos de equipamiento relevante a instalar en el sitio alternativo; conectividad con los sistemas críticos desde el sitio alternativo; acceso a la documentación crítica y directorios de red relevantes; redirección de comunicaciones y otros servicios esenciales hacia el sitio alternativo.

- **Escenarios con impacto en sistemas de información**: Se tomarán decisiones respecto a mecanismos de redundancia y copias de seguridad, procedimientos de backup y recuperación de sistemas de información, suministro redundante de energía, redundancia de la infraestructura de comunicaciones, periodicidad de las pruebas de contingencia, etc. De manera adicional, se deben definir procedimientos manuales de operación por parte de las áreas de negocio para mantener cierta operativa de los procesos críticos, en caso de una caída de los sistemas de información que los soportan.

- **Escenarios con impacto en personas**: Identificación de backups para todos los colaboradores involucrados en tareas del plan de continuidad, establecimiento de programas de formación cruzada, distribución del personal crítico (y sus alternativos) en diferentes localizaciones para minimizar riesgos, definición de procedimientos de contratación de urgencia, etc.

- **Escenarios con impacto en proveedores**: Se debe asegurar que todos los proveedores de servicios identificados como críticos, implanten, mantengan y prueben de forma periódica los planes de continuidad de negocio, para dichos servicios. Se deben incluir cláusulas específicas de continuidad de negocio en los acuerdos de nivel de servicio (ANS) con el proveedor. De manera adicional, se considera la conveniencia de participar o supervisar las pruebas de continuidad del proveedor, de realizar auditorías in situ, de disponer de un proveedor alternativo para el servicio o de asumir

ciertas tareas internamente en el caso de que una contingencia afecte al proveedor, entre otros.

7.4 DESARROLLO DEL PLAN DE CONTINUIDAD DE NEGOCIO (PCN).

Basado en los resultados de las fases descritas anteriormente, la Organización debe garantizar que se desarrolla, se implanta, se mantiene y se prueba periódicamente el plan de continuidad de negocio, considerando los siguientes aspectos:

7.4.1 Procedimientos de gestión de crisis:

Que contemplen las tareas que se deben ejecutar de manera inmediata tras una contingencia (para cada tipo de escenario), condiciones y pasos para activar el PCN, procedimientos de escalamiento, protocolos de comunicación interna y externa (incluyendo accionistas, clientes, proveedores, reguladores y otras terceras partes interesadas) y una estructura de supervisión para coordinar y dar soporte a las tareas de recuperación. Los procedimientos de gestión de crisis priorizarán la integridad física de las personas, el mantenimiento de la liquidez de la Organización, la salvaguarda del buen nombre y la reputación.

7.4.2 Planes de recuperación de negocio:

Los cuales deben ser definidos para todas las áreas de negocio de la Organización. Estos planes deben describir las tareas, procedimientos y responsabilidades para dar respuesta a los escenarios de contingencia identificados, con el fin de asegurar la pronta recuperación de los procesos críticos, reduciendo al mínimo el impacto de las interrupciones de servicios y las pérdidas financieras. Además, las áreas soporte3 deben definir planes de contingencia, que contemplen las actividades que deben realizarse para apoyar la recuperación de los procesos críticos.

7.4.3 Organización del SGCN:

Se deben asignar roles y responsabilidades para la gestión de continuidad de negocio conforme a los criterios descritos en la presente política.

7.4.4 Protocolo de Comunicación:

Se debe definir procedimientos para comunicaciones internas y externos (clientes, proveedores, reguladores, accionistas y otras partes interesadas) en los que se especifiquen los portavoces autorizados, las directrices para comunicar en función de la audiencia a la que vaya dirigido el mensaje, canales, mensajes predefinidos, etc.

[3] Roles y responsabilidades del SGCN

7.4.5 Plan de Formación:

Se requiere, definir un programa de capacitación anual, incluyendo sesiones de entrenamiento adecuados para las personas que participan en actividades del PCN e iniciativas específicas para concienciar a los colaboradores sobre sus responsabilidades en el ámbito de continuidad del negocio.

7.4.6 Plan de Pruebas:

Todos los planes de recuperación de negocio (considerando los diferentes escenarios de contingencia identificados) se deben probar al menos con periodicidad anual.

Las pruebas deben ser completas y exhaustivas, lo que significa que su alcance debe cubrir escenarios completos en lugar de planes individuales de las áreas de negocio.

En cuanto a las pruebas de DRP (pruebas de contingencia de Tecnología), todos los sistemas críticos identificados en el análisis BIA deben ser testados anualmente por la Dirección de Tecnología, con el acompañamiento del Especialista en Seguridad de la Información o quien haga sus veces. Como excepción, si no es posible probar todos los sistemas críticos en un año, se establecerá una prioridad para garantizar que los sistemas más críticos (RTO inferior a 24h) se prueban, al menos, anualmente y el resto se incluyen en un plan de pruebas bienal. Por otro lado, las áreas de negocio tienen que participar en las pruebas de Tecnología.

En cuanto a los escenarios que afectan a los proveedores críticos, se establecen los controles adecuados para garantizar que estos ponen a prueba sus PCN de manera regular (al menos anualmente), recopilando las oportunas evidencias al respecto.

De manera adicional, si se ha establecido algún plan internamente como una respuesta a ese tipo de contingencia, se deberá incluir una prueba para ese este dentro del plan de pruebas de la Organización.

- La Organización definirá su plan de pruebas anual especificando el alcance de cada prueba, los responsables de su seguimiento, el tipo de prueba y la fecha estimada de ejecución.
- El plan de pruebas y las principales conclusiones extraídas de las pruebas realizadas deben presentarse a la Administración de la Organización, al menos, con periodicidad anual.

7.5 PROCEDIMIENTO DE MANTENIMIENTO DEL PCN

- Es esencial para asegurar la vigencia del plan a través del tiempo y su adaptación a los posibles cambios en la Organización**.**
- La gestión y mantenimiento del PCN debe entenderse como un proceso continuo que refleja los cambios de en la Organización, procesos, ubicaciones, tecnología, entre otros.
- El proceso de análisis de impacto de negocio (BIA) se revisará, en el momento de que se produzca un cambio importante en la Organización.
- Los planes de recuperación y los planes de contingencia serán revisados, por lo menos, anualmente y/o en el momento de un cambio importante en la Organización y/o después de la detección de deficiencias o carencias, como resultado de alguna prueba del PCN. Los resultados de estas revisiones deberán consignadas en un informe que será remitido a la Administración.
- Las estrategias de continuidad y la organización del PCN se revisarán, al menos, anualmente y/o en el momento de un cambio importante en la Organización.

7.6 SEGUIMIENTO Y MEJORA CONTINUA DEL SGCN

La Organización determina:

- La necesidad de ser monitoreado y medido para cumplir con la política y los objetivos de esta.
- Cómo se realiza la medición: métodos para monitoreo y análisis.
- Cuando se debe realizar el monitoreo, la medición y el análisis.

8 DOCUMENTOS DE REFERENCIA

DG-0220 Análisis de impacto de negocio (BIA)

9 CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO

1	15/10/2021	Creación del documento. Definición de lineamientos de Continuidad de Negocio para Proindesa y sus sociedades administradas.

10 FIRMAS DE REVISIÓN Y APROBACIÓN

Elaborador por:	**Revisado por:**			**Aprobado por:**
FIRMADO EN ORIGINAL	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**
ASISTENTE DE PROCESOS	**DIRECTOR DE RIESGOS**	**DIRECTORA DE TECNOLOGÍA**	**DIRECTORA ADMINISTRATIVA**	**VICEPRESIDENTE ADMINISTRATIVA Y FINANCIERA**
Lilian Arriero Barreto	Margarita Ramírez Herrera	Johanna Ardila Cagua	María Helena Cerón David	Vanessa Garay Guzmán

Documento aprobado en la sesión de Junta Directiva No. 119 de Proindesa del 15 de octubre de 2021