Asegurar que Hubemar SAS esté preparado para responder a emergencias, recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios críticos para la atención de clientes y la operación.

**PLAN DE CONTINUIDAD DEL NEGOCIO**

**PLAN DE CONTIGENCIA**



1. **INTRODUCCIÓN**

Hubemar S.A.S reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad de la organización.

La Administración del Plan de Continuidad de Negocios es la política que el Hubemar SAS implementa, para responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos.

El Plan de Continuidad del Negocio es una herramienta que mitiga el riesgo de no disponibilidad de los recursos necesarios para el normal desarrollo de las operaciones y como tal hace parte del Sistema de Gestión de Riesgo Operativo, ofreciendo como elementos de control la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

# OBJETIVOS

## OBJETIVO GENERAL

Asegurar que Hubemar SAS esté preparado para responder a emergencias, recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios críticos para la atención de clientes y la operación.

## OBJETIVOS ESPECIFICOS

* + 1. Lograr un nivel de preparación frente a incidentes que permita asegurar que puede proteger la integridad de las personas y bienes de la entidad en forma adecuada, realizando una buena administración de la crisis.
    2. Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.
    3. Asegurar una pronta restauración de las operaciones afectadas por el evento.
    4. Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.
    5. Cumplimiento de los requerimientos de normas emitidas por la Superintendencia Financiera de Colombia.

1. **ALCANCE**

La Administración del Plan de Continuidad de Negocios es una disciplina que prepara a la organización para poder continuar operando durante un incidente o desastre, a través de la implementación de un plan de continuidad, el cual contempla los lineamientos de administración de la continuidad de la organización , el desarrollo de fases que componen el plan de continuidad y las metodologías definidas por **HUBEMAR SAS** para su ejecución, como también el desarrollo de los planes de contingencia, que se realizan de acuerdo con las prioridades establecidas por la empresa.

De la misma manera, el desarrollo de los planes de continuidad se apoya en las capacidades con las que cuenta el **HUBEMAR SAS** para enfrentar situaciones que amenacen o afecten la integridad física de sus colaboradores e instalaciones, tales como el Plan de Manejo de Emergencias, los mecanismos de protección y seguridad, Manual de gestión de la comunicación en situaciones de crisis y los demás sistemas de gestión.

1. **CONCEPTOS BASICOS**

**Administración del Plan de Continuidad de Negocios:** Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.

Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

**Incidente de Trabajo:** Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

**Problema de Continuidad de Negocio**: Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

**Planes de contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

**Plan de Continuidad de Negocio (PCN**): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción1.

**Plan de Recuperación de Desastres (DRP):** 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.

**Análisis de Impacto del Negocio (BIA):** Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

**Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso2.

**Amenaza:** Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

**Vulnerabilidad:** Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

**Riesgo:** Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.

**Frecuencia:** Estimación de ocurrencia de un evento en un período de tiempo determinado*.* Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

**Impacto:** Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad.

**Control:** Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

**Riesgo inherente:** Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

**Riesgo residual:** Riesgo remanente tras la aplicación de controles.

1. **CAUSAS DE INTERRUPCION**

Los planes de contingencia se definen de acuerdo con las causas de las posibles interrupciones y a partir de ellas se referencian las acciones a seguir en caso que las mismas se presenten. Estas se pueden unificar en los siguientes escenarios:

* **Ausencia de Personal:** Se presenta cuando el funcionario que ejecuta el proceso no puede asistir a trabajar para desarrollar las actividades propias de su cargo.
* **No acceso al sitio normal de trabajo:** Se presenta cuando por algún evento como desastre natural, enfermedad contagiosa, actividad terrorista, problemas de transporte, huelgas, entre otros, el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo. En este caso y con el ánimo de no interrumpir la operación del proceso crítico se debe contar con un sitio alterno de trabajo, el cual puede ser:
* **Caída de los sistemas tecnológicos:** Se presenta cuando el hardware y/o software presenta falla(s) o cuando haya interrupción prolongada de las comunicaciones, ocasionados por: datos corruptos, fallos de componentes, falla de aplicaciones y/o error humano.
* **No contar con los Proveedores Externos**: Se presenta cuando una o varias actividades del proceso crítico son realizadas por el proveedor y cualquier falla de éste, generaría la no realización efectiva del proceso. En este caso se debe garantizar que en el contrato con el proveedor se especifique la existencia de un Plan de Continuidad del Negocio documentado, adicional, sea probado en conjunto con los colaboradores de la Entidad y aprobado por HUBEMAR SAS.

1. **LINEAMIENTOS**

El objetivo de la administración de continuidad del negocio es planificar las acciones necesarias para responder de forma adecuada ante un incidente de trabajo, desde el momento en que se declare la contingencia hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

Los lineamientos se sustentan en un conjunto de principios que han sido formulados basándose en las necesidades del negocio y en el entendimiento de los riesgos asociados, ellos son:

* + 1. El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.
    2. Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Contingencia del Negocio.
    3. En caso de presentarse un incidente significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos, de acuerdo con el manual de Comunicación en Situaciones de Crisis.
    4. Los Jefes de área deben designar un Líder de Plan de Continuidad del Negocio, quien es responsable de apoyar las actividades del Programa de Plan de Continuidad de Negocios para el área que representa.
    5. Las diferentes etapas que conforman la fase de Prevención deben ser ejecutadas con la siguiente frecuencia:
* El análisis de impacto del negocio debe actualizarse cada dos (2) años o cada vez que un Líder de Proceso lo requiera, teniendo en cuenta los cambios del Instituto y sus necesidades.
* El monitoreo a los riesgos de continuidad se efectuará de manera semestral.
* Pruebas anuales deben realizarse a todas las estrategias de contingencia definidas.
* Las estrategias se revisarán cada vez que el Líder del Proceso lo considere o como resultado del análisis de riesgos se determine el ajuste o implementación de estrategias de contingencia.
  + - * Los procesos críticos deben ser recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad del Negocio.
      * La Entidad ha definido como el nivel máximo de aceptación del riesgo residual, la clasificación de Tolerable.
      * Los procesos / servicios de la organización que sean desarrollados por terceros contratados deben disponer de planes de continuidad, para lo cual el funcionario interventor del contrato debe solicitar este documento y remitirlo a la Oficina de sistema de gestión, donde se analizará la cobertura del mismo. Adicionalmente, se debe verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas, donde la Oficina de Riesgos debe coordinar con el área responsable del contrato la ejecución de pruebas a dicho plan.
      * Los planes de contingencia deben mantenerse actualizados, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, proceso, tecnología; siendo necesario que en dicha revisión participen las áreas involucradas.

1. **NORMAS EXTERNAS**
   * + - Circular 038/2009 – Sistema de Control Interno: Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad para responder a las fallas e interrupciones específicas de un sistema o proceso y capacidad de retorno a la normalidad.
       - Circular 042/2012: Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.
       - Además, existen metodologías del Plan de Continuidad del Negocio fundamentado en el uso de buenas prácticas reconocidas y normas internacionalmente aprobadas basadas en la gestión de riesgos, entre ellas se encuentran DRI International (Disaster Recovey Institute International) e ISO 22301, ISO27001, las cuales fueron tenidas en cuenta para la elaboración de este documento
2. **ESTRUCTURA DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO**

Para asegurar una adecuada administración de la continuidad del negocio se estableció un estructura, que incluye la definición de los roles y responsabilidades, tanto de los Líderes de Proceso, como de la Alta Gerencia. Esa administración está conformada por:

|  |  |
| --- | --- |
| **COMITÉ** | **ROLES DE CONTINGENCIA** |
| GERENTE ADMINISTRATIVO Y FINANCIERO | Director de Continuidad |
| COORDINADOR SGI | Líder de Administración /Recuperación Infraestructura Física |
| COORDINADOR TIC´S | Líder de Recuperación Tecnológica y Comunicaciones |
| BRIGADA DE EMERGENCIA | Coordinadores de Recuperación |

* + - 1. **ROLES Y RESPONSABILIDADES**

A continuación se describen los roles y responsabilidades de los integrantes del Comité en lo respectivo al plan de continuidad; vale aclarar las personas nombradas como principales y sus suplentes (alternos) tienen las mismas responsabilidades.

**Director de Continuidad**

El Director de Continuidad es el encargado de dirigir y liderar todas las actividades del plan de continuidad del negocio. Es responsable de declarar la contingencia ante el escenario de interrupción de lugar de trabajo.

Responsabilidades.

* + - * + Evaluar y aprobar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la entidad..
        + Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad.
        + Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.
        + Velar por la seguridad del personal que actúa en el área del evento.
        + Establecer los objetivos de recuperación y activar el plan de continuidad ante el escenario de interrupción de lugar teniendo en cuenta el resultado de la evaluación
        + Velar por la ejecución del debido análisis causa – raíz del evento que ocasionó la contingencia.

**Coordinador SGI**

El Coordinador SGIayuda a coordinar los aspectos logísticos internos cuando la Entidad se encuentre operando bajo contingencia. Es quien ayuda a gestionar en cada una de las instalaciones el suministro de elementos esenciales para asegurar el desarrollo de la operación.

Responsabilidades

* + - * + Coordinar el suministro de elementos esenciales como transporte, recursos de infraestructura y papelería.
        + Gestionar la consecución y adecuación de los centros alternos de operaciones según el plan de operaciones en contingencia.

**Coordinador TIC´S**

Es la persona encargada de liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. Es el contacto directo entre la Dirección además, apoya las decisiones tomadas por el Director de Continuidad durante la declaración y activación de la contingencia.

Responsabilidades

* + - * + Liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas.
        + Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad..
        + Colaborar en la comunicación a los proveedores de los temas o servicios de su competencia, sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Director de Continuidad, mediante comunicado elaborado en conjunto con la Oficina Asesora de Comunicaciones.
        + Velar por la actualización de la Estrategia Tecnológica en los casos que se presenten situaciones como: cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros.
        + Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en las mismas.
        + Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

**Brigadas de emergencias**

Las brigadas de emergencias son personas encargadas de liderar la recuperación de procesos de negocio críticos, basados en las estrategias de contingencia. Son el contacto directo entre los procesos de negoci

Responsabilidades

* + - * + Liderar las reuniones del equipo de recuperación, para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.
        + Ejecutar los planes de contingencia ante el incidente presentado.
        + Identificar los posibles riesgos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad.
        + Mantener comunicación constante durante el estado de contingencia.
        + Colaborar en la comunicación a los proveedores sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Director de Continuidad, mediante comunicado elaborado en conjunto con la Oficina Asesora de Comunicaciones.
        + Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en la misma.
        + Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

1. **ENTRENAMIENTO**

En el éxito del Plan de Continuidad es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. La administración de continuidad debe asegurar que todos los funcionarios involucrados reciban entrenamiento sobre los procedimientos a seguir en caso de incidentes o desastres, lo cual permite tomar conciencia de la importancia del plan, ya que serán los encargados de ponerlos en funcionamiento en caso de presentarse un evento no deseado. A los Jefes de las áreas también se les capacita y concientiza, ya que son los responsables de la correcta ejecución de los planes.

Dentro de la política de capacitación se contempla suministrar a todos los funcionarios capacitación anual de Plan de Continuidad de Negocios.

*Anexo Plan de Formación*

1. **DESARROLLO**

|  |  |  |  |
| --- | --- | --- | --- |
| **SITUACIONES O RIESGOS POSIBLES** | **PLAN DE CONTINGENCIA  (Espacio para describir las actividades definidas por el proveedor)** | | |
| **ACTIVIDADES ANTES DEL EVENTO** | **ACTIVIDADES DURANTE EL EVENTO** | **ACTIVIDADES DESPUES DEL EVENTO** |
| **ELEMENTOS BASICOS** |
| TERREMOTO | mantenimiento de la infraestructura, simulacro, preparación de las brigadas emergencias, correos electrónicos de recomendaciones | Activación del plan de emergencia | hacer efectivas las pólizas de seguros, inversiones necesarias para reponer las perdidas (equipos, maquinaria, edificaciones, terrenos etc) |
| INUNDACION | Análisis de las características del terreno, edificación, verificación de tuberías, monitoreo de diques y caudales de los rios cercanos en el caso que aplique | Active el plan de crisis, emergencias (actividades organizadas y concertadas para atender la situación de emergencia) | hacer efectivas las pólizas de seguros, inversiones necesarias para reponer las perdidas (equipos, maquinaria, edificaciones, terrenos etc) |
| INCENDIO | Inspección diaria de la infraestructura, simulacro, preparación de las brigadas emergencias, correos electrónicos de recomendaciones, | Active el plan de crisis, emergencias (actividades organizadas y concertadas para atender la situación de emergencia | hacer efectivas las polizas de seguros, traslado hacia las oficinas de Serpomar y DBP para continuar con la operación |
| CORTE DE ENERGIA | Inspecciones mensuales a la subestación eléctrica, y a la fuente auxiliar (combustible, nivel aceite) monitoreo suspensiones electricas programadas (envio previo reporte proveedor) | Inicio fuente auxiliar de energía auxiliar y cambio desde la red primaria, monitoreo (estado combustible, aceite y temperatura normal de funcionamiento) se verifica la causa del corte (externa o interna) | Se verifica estabilidad de la red eléctrica primaria, si lo está se pasa de auxiliar a red primaria. Se apaga energía auxiliar. Se verifica estado de equipos eléctricos y electrónicos. En caso de falla por causa interna, se hacen correctivos. En caso de falla de algún equipos, se ejecutan las polizas de seguro necesarias para reponer la pérdida |
| CIBER ATAQUES | Revisión periódica para encontrar si hay puntos débiles en la seguridad perimétrica de la red (firewall). Bloque sitios no deseados (redes sociales, videos, p2p), copias de seguridad de la información plataformas principales ubicadas en datacenters con certificación ISO27001. Actualización software perímetrico última versión disponible | Bloqueo total de emergencia (nada entra, nada sale), desconexión física de la red pública | Verificación tipo de ataque y fuente para parcheo. Verificación de la integridad de la información y restauración última copia protegida en caso de requerirse. Notificación a la autoridad competente |
| FALLAS EN LAS COMUNICACIONES | Verificación funcionamiento equipos de comunicaciones, funcionamiento enlaces principales y de backup | Se activan canales de comunicación de respaldo hasta que se normalice la situación. Se contactan a los proveedores mediante los canales habilitados para ellos para solución | Se restablecen comunicaciones principales. En caso de falla de un equipo interno, se hace cambio inmediato del mismo o se reconfigura según el caso. En caso de falla externa, se revisa si la misma está dentro del acuerdo de nivel de servicio |

1. **ESTRATEGIA Y DESCRIPCIÓN RESUMIDA**

Factor Clave de Continuidad Operativa

* Nuestros servicios son esencialmente de gestión documental, de coordinación, de trazabilidad e información.
* Factor clave: flujo controlado de información y documentos, administrados por personas y sistemas

1. **PILARES CLAVE DE CONTINUIDAD**

* Procesos y sus flujos altamente automatizados y estandarizados.
* Personal altamente entrenado en dichos procesos estandarizados
* Poderosos sistemas informáticos de desarrollo externo con un proveedor certificado, que soportan la operación automatizada, así como su visibilidad y trazabilidad.
* Plataforma redundante alojada en centros de datos de alta seguridad

1. **PRINCIPALES CARACTERÍSTICAS DE CONTINUIDAD DE NUESTROS PROCESOS**

* La información y trazabilidad de cada operación está en el sistema, en forma redundante, administrada y respaldada. NO está en papeles o en la cabeza de algún empleado, ni en discos de PC.
* Los documentos relevantes de cada operación de cada cliente están digitalizados en el sistema y son accesibles en línea
* El sistema opera desde Data Center externo de alto nivel de seguridad y disponibilidad, y site de contingencia redundante (Tier 3).
* Cualquier persona faltante en la operación puede ser fácilmente reemplazada por otra de perfil similar en cualquier momento.
* Sistemas accesibles a través de cualquier conexión de Internet, incluso de baja velocidad o acceso a través de banda ancha móvil. Y teléfonos celulares
* Sites de continuidad de negocios (oficinas alternativas) preparados para llevar a ellos la operación en caso de siniestro en nuestras oficinas principales o sucursales.
* Ubicuidad / Adaptabilidad de Operación ante Condiciones Adversas
* Capacidad probada de montar en forma rápida y simple un sitio alternativo para realizar operaciones
* Organigrama accesible vía WEB, permanentemente al día, con claros procedimientos de reemplazo ante personal faltante.
* Líderes de reemplazo reconocidos y entrenados se hacen cargo de la operación ante ausencia de los titulares según lo indicado en Organigrama en línea.
* Comunicación de emergencia por voz:
* Todo nuestro personal clave cuenta con celulares corporativos
* Actualmente, la organización cuenta con equipos de computo de última generación (El parque informático tiene un promedio de edad de 1 año).
* Todas nuestras oficinas donde Hubemar tiene presencia, cuentan con internet dedicado en fibra óptica como canal principal, y una conexión en HFC (Hybrid Fibre Coaxial) como respaldo en caso de que los canales principales fallen. Nuestros sistemas de interconexión cuentan con auto failover, lo que permite hacer cambios automáticos de canal principal a respaldo de manera imperceptible al usuario.
* Para el manejo de nuestras plataformas (IB, Imágenes, FileServer), contamos con robustos servidores de última generación, configurados para altas cargas transaccionales y con sistemas de redundancia, tanto en discos (RAID 5) como en energía (fuentes redundantes).
* Adicionalmente, para nuestra plataforma I-B, columna vertebral de Hubemar (después del talento humano), contamos con un servidor de respaldo, de manera que en una improbable falla catastrófica del servidor principal, en más tardar una hora, podemos poner a funcionar el backup y así continuar la operación.
* Todas nuestras bases de datos son respaldadas al menos dos veces al día y almacenadas fuera de las premisas de Hubemar, según los estándares del BASC.
* Todo lo anterior se encuentra protegido con uno de los sistemas de seguridad perimetral basados en BSD, más robustos existentes. Concretamente el pfSesne. Nada entra, nada sale sin nuestra autorización.
* Tanto servidores, como racks de comunicaciones, switches, módems, transceptores, etc, cuentan con sistemas ininterrumpidos de energía (UPS). Adicionalmente, contamos con planta eléctrica de emergencia. Todo lo anterior para tener nuestros sistemas informáticos disponibles 24x7x365 y así dar continuidad al negocio.
* Cada uno de nuestros funcionarios cuenta con una línea celular, estando disponible casi las 24 horas del día. Adicionalmente muchos de ellos tienen smartphones, lo que les permite también dar celeridad a sus solicitudes hechas de manera electrónica