Tabla de contenido

1. OBJETIVO 4

2. ALCANCE 4

3. DEFINICIONES 4

4. POLÍTICAS 5

5. CONDICIONES GENERALES 5

5.1 Recursos 5

5.1.1 Elementos Para Atender Emergencias 5

5.1.2 Recurso Humano 6

5.2 RESPONSABILIDADES 7

5.2.1 De la Gerencia General 7

5.2.2 De los Responsables de Continuidad del Negocio 7

5.2.3 Del Coordinador de Salud Ocupacional 8

5.2.4 Del Comité de Contingencia y Continuidad 8

5.2.5 Del Comité Interno de Emergencias 9

5.2.6 De la Dirección de Gestión Humana 9

5.2.7 De los Gerentes, Directores, Jefes de Servicio, Líderes, Coordinadores y Supervisores 9

5.2.8 Del personal de Soporte Técnico e Infraestructura o el tercero que haga sus veces 9

5.2.9 Del Área de Tecnología 10

5.2.10 Del Grupo de Disponibilidad 10

5.2.11 De la Brigada de Emergencia 10

5.2.12 Del Área de Infraestructura Física 10

5.2.13 De todos los empleados de OIGAME CONSULTORES EMPRESARIALES SAS 11

6. ANÁLISIS Y EVALUACIÓN DE RIESGOS QUE AFECTAN LA CONTINUIDAD DE NEGOCIO Y DESCRIPCIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES (DRP): 11

6.1. Identificación de Riesgos 11

6.2. Factores de Riesgo y Tipo De Impacto 12

6.3. Estándar de Evaluación y Tratamiento de los Riesgos 12

6.3.1. Evaluación del Riesgo sin Controles (Riesgo Inherente) 12

6.3.2. Tratamiento del Riesgo Inherente 13

6.4. Control del Riesgo 13

6.5. Evaluación del Riesgo Residual 13

6.6. Niveles de Aceptación del Riesgo después de Controles ... 13
6.7. Monitoreo del Riesgo Residual ... 14
6.8. Revisión y actualización del Análisis de Riesgos ... 14
7. PLAN DE PREVENCIÓN ... 14
7.1. Mantenimientos de Infraestructura Física ... 14
7.2. Mantenimiento de Infraestructura Tecnológica ... 14
7.3. Sensibilización y Capacitaciones ... 15
8. PLANES DE EMERGENCIA Y CONTINGENCIA ... 15
8.1. Emergencia y Contingencia ... 15
8.2. Planes de Emergencia OIGAME CONSULTORES EMPRESARIALES SAS ... 15
8.2.1. Protocolo General de Acción en una Emergencia ... 15
8.3. Plan de Contingencia ... 16
8.3.1. Categorías de Contingencia ... 16
9. PROTOCOLO DE COMUNICACIÓN EN CRISIS ... 16
9.1 Declaración del Estado de Emergencia o Contingencia. ... 16
9.2 Aviso a Personal. ... 16
9.3 Aviso a Proveedores. ... 17
9.4 Aviso a Clientes ... 17
9.5 Declaración de retorno a la normalidad ... 17
10. PLAN DE CONTINUIDAD Y EJECUCIÓN DEL DRP ... 17
10.1 Estrategia de Ubicación Física de las Áreas/Procesos/Negocios en caso de requerir continuidad de la operación en otra instalación. ... 17
10.2 Estructura Mínima para la operación en momentos de Contingencia ... 18
10.3 Escenarios de Riesgo y Estrategias de Contingencia para dar continuidad al servicio ... 19
10.4 Tiempos Máximos Tolerables de Interrupción (MTPD) y Tiempos de Recuperación Objetivo (RTO) ... 19
11. PLAN DE CONTINGENCIA, CONTINUIDAD Y DRP ESPECÍFICO POR ÁREA, PROCESO O NEGOCIO ... 21
12. PLAN DE RETORNO A LA OPERACIÓN NORMAL ... 22
12.1 Recuperación Tecnológica ... 22
12.2 Recuperación Operativa ... 22
12.3 Recuperación de Documentos/Archivos ... 22
12.4 Procedimiento de tratamiento y recuperación de documentos físicos afectados por un incidente (documentos sueltos, en carpetas, en AZs, en cajas, etc.) ... 22

12.5 Procedimiento de tratamiento y recuperación de medios magnéticos afectados por un incidente (Cds, Cintas, Rollos de microfilm, Cartridges, Videos, Tapes backup) 23

13. RETROALIMENTACIÓN 24

13.1 Análisis y Evaluación del Incidente 24

13.2 Análisis de Pérdidas de Información 24

13.3 Evaluación de Resultados 24

14. PLAN DE PRUEBAS DEL PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO 24

15. PLAN DE CONTINGENCIA EN CASO DE OCURRENCIA DE EVENTOS O DESASTRES EN LAS INSTALACIONES DEL CLIENTE DONDE OPERA OIGAME CONSULTORES EMPRESARIALES SAS 25

16. PÓLIZAS 25

17. ANEXOS 26

17.1 Personas con Disponibilidad para Fines de Semana 26

17.2 Listado de Proveedores a Contactar en Momentos de Contingencia 26

18. MAPA CONCEPTUAL 27

19. CONTROL DE CAMBIOS 27

ANUNCIO DE CONFIDENCIALIDAD

El presente documento es de carácter confidencial y está protegido por las normas de derechos de autor, cualquier reproducción, distribución o modificación total o parcial a usuarios no autorizados o cualquier uso indebido de la información confidencial podrá ser considerado incidente conforme a lo establecido en los artículos 148 a 258 y 431 del Código Penal Colombiano.

Este documento es el resultado de un trabajo desarrollado por IGAAC (International Group of Advising, Audit and Control Colombia S.A.S) para atender las necesidades de OIGAME CONSULTORES EMPRESARIALES SAS. Su contenido no debe ser revelado, duplicado, usado o publicado total o parcialmente, fuera de la organización, sin la autorización expresa escrita de IGAAC.

1. OBJETIVO

Garantizar la continuidad de los procesos establecidos y servicios ofrecidos por OIGAME CONSULTORES EMPRESARIALES SAS que se vean afectados por desastres naturales o provocados por el ser humano, asegurando la disponibilidad de la información propia y de nuestros clientes.

2. ALCANCE

Este Plan de contingencia, continuidad y DRP del negocio cubre a todos los procesos de OIGAME CONSULTORES EMPRESARIALES SAS, desarrollados en cualquiera de sus instalaciones a nivel nacional.

3. DEFINICIONES

- **BCM (Business Continuity Management):** Administración de la Continuidad del Negocio. Proceso administrativo completo que identifica impactos potenciales que puedan afectar la organización. Provee la estructura para dar flexibilidad y respuestas efectivas para salvaguardar los intereses de la organización.
- **BCP (Business Continuity Plan):** Plan de Continuidad del Negocio. Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de negocio generando un impacto mínimo ante un incidente.
- **Brigada de Emergencias:** Acciones coordinadas desarrolladas por un grupo de personas de una Compañía, organizadas, entrenadas y equipadas especialmente para responder a las emergencias.
- **Contingencia:** Evento que ocasiona la detención parcial o total de uno o varios procesos y que obliga a planes alternos de operación para dar continuidad al servicio. En OIGAME CONSULTORES EMPRESARIALES SAS se definieron tres tipos de contingencias: Contingencia Leve, Media y Crítica.
- **Contingencia Crítica:** Aquella que afecta a uno o varios Procesos de la Compañía, generando la suspensión de estos, involucrando la integridad de los empleados o personas que están en el área y compromete a la Compañía en acciones de mayor impacto. Serán manejadas por la Brigada de Emergencia, Grupo de Disponibilidad si compete a fin de semana, Comité de Contingencia y Comité de Gerencia.
- **Contingencia Media:** Aquella que afecta a uno o varios Procesos de la Compañía, generando la suspensión de estos, sin involucrar la integridad de los empleados o personas que están en el área. Serán manejadas por la Brigada de Emergencia, Grupo de Disponibilidad si compete a fin de semana y Comité de Contingencia.
- **Contingencia Leve:** Aquella que solo afecta una actividad dentro de un Proceso de la Compañía, y que no involucra la suspensión del Proceso completo, ni la integridad de los empleados o personas que están en el área, ni compromete a la Compañía. Serán manejadas por el personal o área afectada y el área de Seguridad.
- **CIEC:** Comité Interno de Emergencias y Contingencias
- **Desastre:** Es el resultado de una emergencia, cuyas consecuencias puedan considerarse de carácter grave para el Sistema que las sufre.
- **DRP (Disaster Recovery Plan):** Plan de Recuperación de Desastres. Estrategias definidas para asegurar la reanudación oportuna y ordenada de los servicios informáticos críticos en caso de contingencia. **También llamado Plan de Contingencia y Continuidad Tecnológico**.
- **Emergencia:** Toda situación que implique un "estado" de perturbación parcial y/o total de un "Sistema" por la posibilidad u ocurrencia real de un siniestro y cuya magnitud puede poner en peligro la estabilidad del mismo.
- **EMR:** Estructura Mínima Requerida para operar en momentos de contingencia.
- **Evacuación:** Acción planificada mediante la cual cada persona amenazada por riesgos colectivos desarrolla procedimientos predeterminados, tendientes a ponerse a salvo por sus propios medios o por los existentes en su área, mediante el desplazamiento desde y hasta lugares de menor riesgo.

- **Responsables de la Continuidad de Negocio:** Personal involucrado de OIGAME CONSULTORES EMPRESARIALES SAS encargado de construir, implementar y divulgar la estrategia de Continuidad de Negocio de la Compañía.
- **Mantenimiento Preventivo:** Inspección periódica que se realiza para evaluar el estado de funcionamiento de la infraestructura e identificar fallas, además de prevenir y mantenerla en condiciones óptimas para su funcionamiento.
- **Mantenimiento Correctivo:** Corrección de averías o fallas cuando estas se presentan.
- **Plan de Contingencia y Continuidad del Negocio:** Plan de Contingencia y Continuidad del Negocio
- **Plan de Emergencias**: Requerimientos generales de orden organizativo, técnico y operacional que deben cumplirse en todas las instalaciones de la Compañía, con el fin de responder a las posibles emergencias que puedan presentarse.
- **Plan de Recuperación o Continuidad:** Acciones a llevar a cabo para retornar a la normalidad de las operaciones luego de ocurrida una contingencia.
- **Prueba Operativa:** Es la prueba que contempla simular contingencia en el funcionamiento normal de la operación en sus instalaciones regulares, motivo por el cual se traslada la operación a otra locación física.
- **Prueba Tecnológica:** Es aquella que contempla probar con el área de Tecnología el buen funcionamiento de los aplicativos/sistemas/comunicaciones/redes al ser reinstalados o configurados por contingencia de fallo en sus servicios.
- **Riesgo:** Daño potencial que puede surgir por un proceso presente o futuro. Exposición a la posibilidad de ocurrencia de ciertas cosas tales como pérdida o ganancia de acuerdo a la naturaleza del negocio.
- **RTO:** (Recovery Time Objective) Tiempo de recuperación objetivo. Es el tiempo ideal en el que se espera estar prestando el servicio otra vez, después de una contingencia o emergencia. Algunas veces puede estar establecido contractualmente con el cliente.
- **Seguridad:** Un nivel "aceptable" de riesgo.

4. POLÍTICAS

Este Plan de Contingencia y Continuidad del Negocio se genera soportado en las siguientes Políticas de OIGAME CONSULTORES EMPRESARIALES SAS.

- Política Sistema Integrado De Gestión DG-GGE-005
- Política de Continuidad del Negocio PO-GGE-001

5. CONDICIONES GENERALES

5.1 Recursos

5.1.1 Elementos Para Atender Emergencias

La Gerencia General ha dotado cada una de las sedes de la compañía con los siguientes Elementos para atender emergencias:

- MEGÁFONO, para orientar al personal en el momento de la emergencia.
- CONOS VIALES, para cerrar el espacio de la vía que se utilice al momento de evacuar las instalaciones
- PALETAS DE PARE Y SIGA, para que el personal de seguridad física o de brigadas pueda orientar el paso de vehículos y personas
- CINTA DE DEMARCACIÓN, para encerrar aquellas zonas que se identifiquen como peligrosas
- EQUIPOS PARA ATENCION DE EMERGENCIAS (EXTINTORES, CAMILLAS, BOTIQUIN)

5.1.2 Recurso Humano

Para el funcionamiento del Plan de Contingencia y Continuidad del Negocio de OIGAME CONSULTORES EMPRESARIALES SAS se requiere la participación de todos los empleados de la compañía. Adicionalmente, dentro de la compañía se cuenta con los siguientes grupos de apoyo para el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO:

5.1.2.1 Comité De Contingencia Y Continuidad

OIGAME CONSULTORES EMPRESARIALES SAS cuenta un Comité de Contingencia y Continuidad que se reúne para revisar los aspectos correspondientes al PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO, evaluar los incidentes ocurridos y tomar las decisiones necesarias de prevención y corrección. Dicho comité está conformado por un representante de:

- Gerencia General
- Dirección de Operaciones
- Continuidad del Negocio
- Oficial de Seguridad de la Información
- Infraestructura Tecnológica
- Gestión Humana

A las sesiones del Comité también podrán ser invitados funcionarios de áreas específicas para revisar temas correspondientes a ellas.

El Comité es convocado por los Responsables de la Continuidad del Negocio cuatrimestralmente o de manera extraordinaria por el Oficial de Seguridad de la Información, el líder asignado o por cualquiera de sus integrantes cuando se requiera.

5.1.2.2 Comité Interno de Emergencias y Contingencias (CIEC)

OIGAME CONSULTORES EMPRESARIALES SAS cuenta un Comité Interno de Emergencias, conformado por:

- Un Director de Emergencias
- Un Coordinador de Apoyo Interno y Externo
- Un Coordinador de Comunicaciones
- Un Jefe de Brigada de Emergencia

5.1.2.3 Brigada de Emergencias

OIGAME CONSULTORES EMPRESARIALES SAS cuenta con Brigadas de Emergencia, conformadas por personal operativo y administrativo. Este personal es capacitado por el área de Salud Ocupacional en los temas relacionados con su labor en caso de una Emergencia.

5.1.2.4 Grupo de Disponibilidad para Fines de Semana

Teniendo en cuenta que en los horarios laborales normales de Lunes a Viernes siempre hay presencia de la Brigada de Emergencias, pero que los fines de semana las instalaciones generalmente solo cuentan con el personal de Seguridad Física de turno, el personal administrativo de OIGAME CONSULTORES EMPRESARIALES SAS comprometido con la estabilidad de la compañía, se ha unido en un Grupo de

Disponibilidad que permite tener responsabilidad compartida en cuanto a la actuación ante un evento presentado en las instalaciones de la compañía los fines de semana.

Este Grupo está compuesto por funcionarios de la parte Administrativa o de Operaciones de OIGAME CONSULTORES EMPRESARIALES SAS, quienes de manera rotativa mensual estarán disponibles y de forma presencial (si aplica) los fines de semana para atender situaciones de emergencia o monitoreo en las instalaciones de la compañía, y hacer presencia en las mismas de ser requerido, con el objeto además de dar apoyo al área de Seguridad Física que siempre se encuentra 7x24 en la compañía.

En el momento de una emergencia o contingencia el fin de semana, el personal de Soporte Técnico debe comunicarse inmediatamente con el Director de Emergencias y a su vez con el Grupo de Disponibilidad.

Para el funcionamiento del Grupo de Disponibilidad se tendrán en cuenta las siguientes premisas:

- El GRUPO de Disponibilidad funcionará solo para los fines de semana.
- Cada fin de semana estarán 2 personas disponibles, teniendo en cuenta la cantidad de personal administrativo de la sede.
- Las personas responsables en el fin de semana tendrán que atender las que llegaren a presentarse contingencias.
- Los Responsables de la Continuidad del Negocio velarán porque se informe periódicamente el cronograma general de disponibilidad.
- Los Responsables de la Continuidad del Negocio velará porque se recuerde mensualmente quiénes son las personas disponibles cada fin de semana.
- En el momento en que ocurre la contingencia el fin de semana, el personal de Seguridad Física o el tercero que ejerce esta función, será el encargado de avisar a las personas disponibles y solicitar su apoyo.
- El acceso de las entidades de soporte a las instalaciones debe hacerse previa verificación de la identidad de los funcionarios, sin que esto obstaculice la agilidad en el ingreso para la atención de la emergencia.
- Este es un compromiso del personal administrativo con la compañía. Si el funcionario disponible, tiene algún inconveniente con la fecha en la que ha sido programado, deberá avisar oportunamente los Responsables de la Continuidad del Negocio para el cambio de la fecha.

5.2 RESPONSABILIDADES

5.2.1 De la Gerencia General

Aprobar el Plan de Contingencia, Continuidad y DRP del Negocio apoyado en el Comité de Contingencia y Continuidad, y proporcionar los recursos de tiempo, humanos y de infraestructura necesarios para su efectividad.

5.2.2 De los Responsables de Continuidad del Negocio

- Participar en la redacción el documento del **PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO** y llevarlo para aprobación al Comité de Contingencia y Continuidad.
- Contribuir a mantener actualizada y publicada la documentación sobre el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO.

- Contribuir a la divulgación toda la información necesaria sobre el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO.
- Supervisar que se lleve registro de las contingencias presentadas en la compañía.
- Apoyar o Realizar capacitaciones y sensibilización sobre el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO a toda la compañía.
- Ayudar a Coordinar con los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) las fechas del cronograma de pruebas y realizar las pruebas de contingencia estipuladas.
- Asegurar que se cite a Comité de Contingencia y Continuidad cuando se presenten contingencias para evaluar o tomar decisión, o para discutir temas relacionados con el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO
- Validar que se organice el cronograma de fechas de disponibilidad para el Grupo de Disponibilidad y recordar semanalmente a los disponibles su compromiso.
- Velar por que se mantenga y actualizada la información soporte del Plan de Contingencia y Continuidad de Negocio: Estructura Mínima Requerida, Contactos de Contingencia, Escenarios de Riesgo y Estrategias de Contingencia, MTPO y RTO (Ver el BIA), en conjunto con los jefes de área o negocio.
- Participar en el análisis de riesgos e incluir nuevos riesgos y presentarlos en Comité de Contingencia

5.2.3 Del Coordinador de Salud Ocupacional

- Redactar y mantener actualizado el Plan de Emergencia y Análisis de Vulnerabilidad
- Divulgar a toda la Compañía el Plan de Emergencia y Análisis de Vulnerabilidad
- Realizar capacitaciones y sensibilización sobre el Plan de Emergencia y Análisis de Vulnerabilidad a todo el personal de la compañía y proveedores
- Gestionar la capacitación a las Brigadas de Emergencias
- Citar a los Comités Internos de Emergencia para evaluar situaciones y capacitar a sus integrantes.
- Realizar Simulacros de Evacuación
- Coordinar y divulgar los puntos de encuentro y protocolos de emergencia

5.2.4 Del Comité de Contingencia y Continuidad

- Apoyar al Gerente General en la aprobación del documento del Plan de Contingencia y Continuidad del Negocio y sus actualizaciones
- Resultado de revisiones periódicas en los comités, fortalecer el contenido del PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO
- Apoyar la implementación del PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO, colaborando con capacitaciones y sensibilizaciones.
- Evaluar las contingencias presentadas y definir acciones preventivas o correctivas cuando corresponda.
- Generar actividades para la sensibilización en la Compañía sobre el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO y participar de ellas.
- Son responsables de declarar el estado de emergencia y declarar el retorno a la normalidad, informando de esto a los Jefes de Área (Gerentes, Directores, Coordinador, Supervisor, Jefe de Servicio, Líder) por el medio que sea posible.

5.2.5 Del Comité Interno de Emergencias

- Aplicar sus funciones según el Plan de Emergencia y Análisis de Vulnerabilidad

5.2.6 De la Dirección de Gestión Humana

- Mantener un listado actualizado y copia de seguridad del mismo en otro lugar, del personal existente en la compañía, su ubicación y número de contacto.
- Soportar al área de Salud Ocupacional y Continuidad de Negocio en las capacitaciones que sean requeridas para sensibilizar al personal

5.2.7 De los Gerentes, Directores, Jefes de Servicio, Líderes, Coordinadores y Supervisores

- Mantener un listado actualizado del personal a su cargo, ubicación y número de contacto. Entregar una copia de dicho listado al personal de Soporte Técnico y encargarse de mantenerlo actualizado.
- Motivar e involucrar al personal a su cargo para que participen en las actividades programadas para verificar la efectividad del PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO.
- Avisar al Cliente sobre el estado de emergencia o contingencia, según los contactos estipulados para ello.
- Durante una emergencia o contingencia, deberá comunicarse cada hora con el Cliente para mantenerlo informado sobre el avance de la situación.
- Definir la estructura mínima requerida para operar en momentos de contingencia, e informarla formal y oportunamente a los RESPONSABLES DE CONTINUIDAD DEL NEGOCIO para mantener actualizada.
- Definir los MTPD y RTO de su Área/Proceso/Negocio, e informarlo formal y oportunamente al Cliente y a los RESPONSABLES DE CONTINUIDAD DEL NEGOCIO para su conocimiento.
- Coordinar con los RESPONSABLES DE CONTINUIDAD DEL NEGOCIO las fechas del cronograma de pruebas y realizar las pruebas de contingencia estipuladas.
- Investigar y divulgar a su personal, el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO del cliente en los casos en que exista personal de OIGAME CONSULTORES EMPRESARIALES SAS laborando en sus instalaciones. Gestionar con el cliente, capacitaciones y sensibilización al respecto.
- Actualizar a los Responsables de Continuidad del Negocio sobre los contactos del cliente para el aviso de una contingencia.

5.2.8 Del personal de Soporte Técnico e Infraestructura o el tercero que haga sus veces

- Actuar en momentos de Contingencia según las actividades estipuladas en este PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO, guiados por las instrucciones del Líder de infraestructura.
- Participar de todas las actividades que se desarrollen sobre el Plan de Contingencia y Continuidad del Negocio: capacitaciones, sensibilizaciones, simulacros, pruebas de contingencia.

5.2.9 Del Área de Tecnología

- Definir en conjunto con los Responsables de la Continuidad del Negocio, el Plan de Contingencia Tecnológico.
- Actualizar cuando corresponda, el Plan de Contingencia Tecnológico.
- Llevar a cabo los mantenimientos preventivos y correctivos de la infraestructura tecnológica estipulados en el instructivo IN-TEI-002 Mantenimiento preventivo.
- Divulgar y Capacitar a los usuarios en el Plan de Contingencia Tecnológico.
- Realizar pruebas de contingencia tecnológica, anualmente.
- Participar en las pruebas de contingencia operativas programadas, apoyando la instalación y/o configuración de infraestructura tecnológica necesaria.

5.2.10 Del Grupo de Disponibilidad

- La persona disponible deberá hacer acto de presencia (si aplica) en donde se genere la contingencia para evaluar y/o verificar la situación.
- En caso de tener que atender una contingencia, los funcionarios disponibles deberán brindar una solución de primera mano mientras llegan los refuerzos necesarios.
- En caso de requerirse, la persona disponible deberá comunicarse con los contactos de contingencia para tomar las acciones correctivas pertinentes.
- Los funcionarios disponibles son responsables de autorizar el ingreso de las entidades de apoyo que se requieran para atender la contingencia (bomberos, ambulancias, policía, empresas de servicios, proveedores, etc.).
- Es responsabilidad de la persona disponible, reportar a los Responsables de la Continuidad del Negocio lo sucedido el fin de semana a primera hora del primer día hábil siguiente, para que éste a su vez reporte la situación al Comité de Contingencia.

5.2.11 De la Brigada de Emergencia

- Las Brigadas son grupos de personas organizadas y capacitadas para emergencias, mismos que serán responsables de combatirlas de manera preventiva o ante eventualidades de un alto riesgo, emergencia, siniestro o desastre, dentro de una empresa, industria o establecimiento y cuya función está orientada a salvaguardar a las personas, sus bienes y el entorno de los mismos.
- Tipos de brigadas de emergencia: Evacuación, Primeros Auxilios, Prevención y Combate de Incendios, Comunicación.
- Los Brigadistas tienen como funciones: Ayudar a las personas a guardar la calma en casos de emergencia, Accionar el equipo de seguridad cuando lo requiera, Difundir entre la comunidad del centro de trabajo, una cultura de prevención de emergencias, Dar la voz de alarma en caso de presentarse un alto riesgo, emergencia, siniestro o desastre, Utilizar sus distintivos cuando ocurra un alto riesgo, emergencia, siniestro o desastre o la posibilidad de ellos, así como cuando se realicen simulacros de evacuación, suplir o apoyar a los integrantes de otras brigadas cuando se requiera, Cooperar con los cuerpos de seguridad externos.

5.2.12 Del Área de Infraestructura Física

- Llevar a cabo los mantenimientos preventivos y correctivos de infraestructura, según lo estipulado en el formato FO-TEI-10.
- Durante una emergencia o contingencia, contactar y gestionar las labores de los proveedores necesarios para apoyar la misma.

5.2.13 De todos los empleados de OIGAME CONSULTORES EMPRESARIALES SAS

- Conocer el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO.
- Participar de todas las actividades que se desarrollen en pro de su divulgación: capacitaciones, sensibilizaciones, simulacros, pruebas de contingencia, etc.

6. ANÁLISIS Y EVALUACIÓN DE RIESGOS QUE AFECTAN LA CONTINUIDAD DE NEGOCIO Y DESCRIPCIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES (DRP):

El resultado de la evaluación y valoración de los riesgos identificados en OIGAME CONSULTORES EMPRESARIALES SAS.

El análisis y evaluación de riesgos que afectan la continuidad de negocio en OIGAME CONSULTORES EMPRESARIALES SAS se realizó teniendo en cuenta los siguientes parámetros:

6.1. Identificación de Riesgos

OIGAME CONSULTORES EMPRESARIALES SAS ha identificado los siguientes riesgos como los que pueden afectar la Continuidad del Negocio:

- Accidente contra nuestras instalaciones, accidente de tránsito, aéreo o similar que afecte nuestras instalaciones.
- Atentado Terrorista cualquier actividad delictiva derivada de manifestaciones terroristas o grupos al margen de la ley que afecte nuestras instalaciones.
- Ausencia de Recurso Humano ausencia de recurso por incapacidades, permisos, renuncias, problemas de transporte.
- Condiciones ambientales para custodia de información en condiciones ambientales propias de la región en la que se encuentran ubicadas las instalaciones de la Compañía, que pueden variar, frente a los parámetros normales de humedad relativa y temperatura en los cuales debe almacenarse la información.
- Conmoción Civil manifestaciones, asonadas que afecte nuestras instalaciones y/o no permitan el ingreso del personal o no permitan laborar en la zona.
- Falla de Infraestructura Física daños de equipos de muebles y enseres, instalaciones.
- Falla de Infraestructura Tecnológica daños de equipos de cómputo, escáners, impresoras, servidores, puntos audio y video y demás elementos tecnológicos vitales para la operación.
- Falla en el Transporte problemas mecánicos o de disponibilidad de los vehículos que prestan el servicio a la operación y al cliente.
- Falla en el Correo Electrónico no funcionamiento del correo electrónico que impida la comunicación interna y/o con el cliente.
- Fallo de Aplicativos inconvenientes que no permitan acceder a los aplicativos que requiere la operación para trabajar.
- Fallo de Página Web inconvenientes que no permitan acceder a las páginas web que requiere la operación y los clientes para trabajar.
- Fallo del canal de conexión interrupción de las comunicaciones por el canal (dedicado, ADSL, radio enlace).
- Fallo del fluido eléctrico interrupción del suministro de energía.

- Fallo de la planta telefónica problemas con la planta que no permitan la entrada y/o salida de llamadas.
- Falla en las comunicaciones celulares falla en las comunicaciones celulares que no permiten la comunicación interna o con clientes.
- Incendio propagación de fuego en las instalaciones.
- Inundación filtración de agua en las instalaciones.
- Robo sustracción de elementos o información propia o del cliente.
- Sismo o Terremoto temblor, movimiento brusco de la tierra.
- Ataques Informáticos: violación a las políticas de seguridad informática (plataforma tecnológica) de la compañía, generada por debilidades que son explotadas por agentes externos.

6.2. Factores de Riesgo y Tipo De Impacto

A cada riesgo se le identifican los factores que lo pueden generar y el tipo de impacto que puede ocasionar su materialización, teniendo en cuenta estos parámetros:

- Factores de Riesgo:
  - Humanos
  - Tecnológicos
  - Infraestructura (física)
  - Externos (desastres naturales, terceros)
- Tipo de Impacto
  - Económico
  - Operativo
  - Legal
  - Imagen

6.3. Estándar de Evaluación y Tratamiento de los Riesgos

OIGAME CONSULTORES EMPRESARIALES SAS define los parámetros, evaluación y tratamiento de riesgos en el procedimiento PR-SIG-010 identificación, evaluación Y Control De Riesgo.

6.3.1. Evaluación del Riesgo sin Controles (Riesgo Inherente)

Para la evaluación de los riesgos inherentes se mide su probabilidad frente al impacto, utilizando la siguiente matriz:

			Impacto			
			Menor	Moderado	Importante	Catastrófico
			1	2	3	4
PROBABILIDAD	Casi seguro	1	Medio	Alto	**Crítico**	**Crítico**
	Muy Probable	0,75	Medio	Medio	Alto	**Crítico**
	Probable	0,5	Bajo	Medio	Medio	Alto
	Poco probable	0,25	Bajo	Bajo	Medio	Alto

6.3.2. Tratamiento del Riesgo Inherente

Para definir el tratamiento del riesgo, se deben tener en cuenta las siguientes premisas

- Los riesgos BAJOS se ACEPTAN
- Los riesgos MEDIOS se EVITAN o se MITIGAN
- Los riesgos ALTOS se MITIGAN
- Los riesgos CRÍTICOS se MITIGAN o se TRANSFIEREN

Cualquiera de los tres primeros puede también transferirse en caso de que así lo sugieran o decidan los responsables del proceso, negocio o área. En el caso de los riesgos MEDIOS, ALTOS y CRÍTICOS se deben definir CONTROLES para su tratamiento.

6.4. Control del Riesgo

Los controles que se definen para cada riesgo pueden ser MANUALES, AUTOMÁTICOS o SEMIAUTOMÁTICOS y de tipo CORRECTIVO, PREVENTIVO o DETECTIVO. Luego de definirlos se debe valorar su efectividad. La escala de valoración de efectividad de control se rige por la siguiente matriz:

Efectividad del Control								Implementación
Forma		Tipo		Evidencia		CALIFICACION		CALIFICACION
Automático	4	Correctivo	1	Si	3	**Fuerte**	9 – 10	Implementado
Semiautomático	2	Detectivo	2	No	1	**Moderado**	6 – 8	En Desarrollo
Manual	1	Preventivo	3			**Débil**	1 – 5	No Existe

Todos los controles que después de su valoración resulten DÉBILES deberán tener un Plan de Acción para fortalecerlos, de manera que se busque la mitigación del riesgo.

6.5. Evaluación del Riesgo Residual

Ya identificados los riesgos inherentes y los controles que se han establecido para mitigarlos, evitarlos o transferirlos, nuevamente se realiza una evaluación de los riesgos teniendo en cuenta la misma matriz de evaluación numeral 6.3.1, para obtener un nuevo resultado sobre el Nivel de Riesgo después de Controles.

6.6. Niveles de Aceptación del Riesgo después de Controles

De la misma forma que se menciona en el numeral 6.3.2, los niveles de aceptación del riesgo después de controles se rigen por las siguientes premisas:

- Los riesgos BAJOS se ACEPTAN
- Los riesgos MEDIOS se EVITAN o se MITIGAN
- Los riesgos ALTOS se MITIGAN
- Los riesgos CRÍTICOS se MITIGAN O se TRANSFIEREN

Cualquiera de los tres primeros puede también transferirse en caso de que así lo sugieran o decidan los responsables del proceso, negocio o área.

6.7. Monitoreo del Riesgo Residual

Con el fin de realizar seguimiento al riesgo residual, se establecen responsables y periodicidad de monitoreo al mismo.

6.8. Revisión y actualización del Análisis de Riesgos

OIGAME CONSULTORES EMPRESARIALES SAS realizará anualmente una revisión del análisis de riesgos, con el fin de actualizarlo según corresponda. Esta revisión será realizada por el Responsables de la Continuidad del Negocio y el Comité de Contingencia y Continuidad.

7. PLAN DE PREVENCIÓN

7.1. Mantenimientos de Infraestructura Física

OIGAME CONSULTORES EMPRESARIALES SAS, cuenta con contratos con terceros y personal de la compañía para el Mantenimiento de la Infraestructura tecnológica, detallando las actividades preventivas y correctivas que se realizan para:

- Demarcación y Señalización
- Sistemas de Aire Acondicionado
- Saneamiento Ambiental
- Equipos de Medición de Temperatura y Humedad Relativa
- Extintores
- Sistema de extinción a base de agua (Gabinetes)
- Cubiertas y Bajantes
- Plantas Eléctricas
- Infraestructura de Tecnología
- Iluminación
- Arreglos Varios
- Mantenimiento de Alarmas y detectores
- Sistema de acceso biométrico
- Sistema de Monitoreo
- Sistema de Telefonía IP
- Centro de Procesamiento de Datos (Data Center)

7.2. Mantenimiento de Infraestructura Tecnológica

OIGAME CONSULTORES EMPRESARIALES SAS, cuenta con un formato para el Mantenimiento Preventivo y Correctivo de la Infraestructura Tecnológica FO-TEI-10, en el cual se detallan todas las actividades correspondientes para tal fin.

7.3. Sensibilización y Capacitaciones

OIGAME CONSULTORES EMPRESARIALES SAS cuenta en la Dirección de GESTIÓN DEL TALENTO HUMANO y SIG con un cronograma de Formación y Capacitaciones que contempla sensibilizaciones en cuanto a temas de Plan de Emergencias, Plan de Contingencia y Continuidad del Negocio

8. PLANES DE EMERGENCIA Y CONTINGENCIA

8.1. Emergencia y Contingencia

OIGAME CONSULTORES EMPRESARIALES SAS ha definido que una Emergencia es aquella situación que pone en riesgo la vida de las personas, además de involucrar en algunos casos una contingencia operativa. De otro lado, una Contingencia no involucra la vida de las personas, sino que afecta la disponibilidad del servicio y/o la operación.

8.2. Planes de Emergencia OIGAME CONSULTORES EMPRESARIALES SAS

El área de Salud Ocupacional ha diseñado Planes de Emergencia para cada una de las instalaciones de OIGAME CONSULTORES EMPRESARIALES SAS, los cuales pueden ser consultados en el administrador de documentos. Estos planes cuentan con:

- Análisis general
- Comité Interno de Emergencia
- Protocolos de Emergencia
-

8.2.1. Protocolo General de Acción en una Emergencia

Para casos de Emergencia, OIGAME CONSULTORES EMPRESARIALES SAS ha diseñado un Protocolo de General de Acción en una Emergencia.

- Establecer para nuestra empresa, una política dirigida al campo de la prevención y atención de emergencias, definiendo el compromiso de sus directivas y la participación de los demás estamentos.
- Identificar y priorizar los riesgos que puedan afectar la organización y analizar el porcentaje de vulnerabilidad presente en nuestras instalaciones.
- Identificar acciones enfocadas a mejorar condiciones de riesgo, para disminuir su impacto y reducir el nivel de vulnerabilidad de nuestros trabajadores, colaboradores y visitantes.
- Definir las funciones, responsabilidades y formas de actuar de todas las personas involucradas en el control de emergencias.
- Establecer los procedimientos de actuación en emergencias.
- Divulgar y establecer el plan de formación para todas las personas, sobre los procedimientos establecidos.
- Evaluar a través de simulacros la implementación del Plan de Emergencias.
- Identificar y valorar en forma anticipada, todas las eventualidades que puedan amenazar a las instalaciones y por ende a sus ocupantes.
- Servir como documento de consulta y guía para funcionarios nuevos o antiguos en aspectos de seguridad con el fin de facilitar la implementación de los procedimientos establecidos.

- Brindar una orientación técnica y eficaz que permita adoptar comportamientos seguros en caso de situaciones de emergencia dentro de las instalaciones de la empresa.

8.3. Plan de Contingencia

8.3.1. Categorías de Contingencia

OIGAME CONSULTORES EMPRESARIALES SAS ha definido las siguientes categorías:

Contingencia Crítica: Aquella que afecta a uno o varios Procesos de la Compañía, generando la suspensión de los mismos, involucrando la integridad de los empleados o personas que están en el área y compromete a la Compañía en acciones de mayor impacto. Serán manejadas por la Brigada de Emergencia, Grupo de Disponibilidad si compete a fin de semana, Comité de Contingencia y Comité de Gerencia.

Contingencia Media: Aquella que afecta a uno o varios Procesos de la Compañía, generando la suspensión de los mismos, sin involucrar la integridad de los empleados o personas que están en el área. Serán manejadas por la Brigada de Emergencia, Grupo de Disponibilidad si compete a fin de semana y Comité de Contingencia.

Contingencia Leve: Aquella que solo afecta una actividad dentro de un Proceso de la Compañía, y que no involucra la suspensión del Proceso completo, ni la integridad de los empleados o personas que están en el área, ni compromete a la Compañía. Serán manejadas por el personal o área afectada y el área de Seguridad.

9. PROTOCOLO DE COMUNICACIÓN EN CRISIS

A continuación, se describen las indicaciones a seguir para el aviso sobre las emergencias/contingencias ocurridas en OIGAME CONSULTORES EMPRESARIALES SAS, en cualquier caso.

9.1 Declaración del Estado de Emergencia o Contingencia.

En el momento que se presenta una EMERGENCIA, entra en acción el Plan de Emergencias y el Comité Interno de Emergencias. Por tanto, es el C quien define y declara públicamente a la Compañía el Estado de Emergencia. Esta confirmación la debe hacer el CIEC a los Jefes de Área (incluyendo todos los cargos).

En el momento en que se presenta una CONTINGENCIA, es el Jefe de Área quien informa a las áreas involucradas sobre la misma. En el formato *Contactos en Momentos de Contingencia* se detallan las personas y números de contacto de las áreas de soporte que actúan en el momento de una contingencia. En ese momento el Jefe de Área debe activar el PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO específico definido para su operación.

9.2 Aviso a Personal.

El Jefe Inmediato del grupo de personas involucrado en la emergencia o contingencia en coordinación con su Director o Gerente de Proceso, debe orientar a su personal presente y ausente sobre las acciones que se tomarán para atender la emergencia y/o contingencia y cómo continuarán con la operación. Cada Jefe Inmediato debe contar con un listado del

personal a su cargo y sus números de contacto, del cual debe permanecer una copia en el área respectiva.

9.3 Aviso a Proveedores.

En caso de requerirse, el Gerente, Dueño o Director de Proceso se comunicará con el área el representante del área administrativa para gestionar el apoyo de Proveedores. Quien, será el encargado de coordinar dichos Proveedores. Dichas áreas contarán con un *Listado de Proveedores a contactar en momentos de contingencia.*

9.4 Aviso a Clientes

En caso de que el servicio hacia el Cliente se vea afectado por la emergencia/contingencia, el Gerente o Director de Proceso comunicarán al cliente o delegarán al (Coordinador, Supervisor, Líder) para que se comunique con el mismo.

Esta comunicación debe ser en primera instancia telefónica y vía correo de ser posible.

El Director de proceso/Jefe de área (Coordinador, Supervisor, Líder), deberá comunicarse cada hora con el Cliente para mantenerlo informado sobre el avance de la situación.

9.5 Declaración de retorno a la normalidad

En una Emergencia, el CIEC define si la misma ya ha sido controlada, y confirma a Directores de Proceso (Gerentes, Directores, Coordinador, Supervisor, Líder) quienes a su vez son responsables de dar aviso a su personal y al Cliente.

En una Contingencia, la confirmación de retorno a la normalidad debe ser definida entre los Responsables de la Continuidad, el Jefe de área/negocio/proceso (Coordinador, Supervisor, Líder) y las áreas de soporte involucradas, quienes a su vez son responsables de dar aviso a Directores, Gerentes su personal y al Cliente.

10. PLAN DE CONTINUIDAD Y EJECUCIÓN DEL DRP

Para dar continuidad a la operación de las diferentes áreas de la compañía, se tendrán en cuenta los siguientes aspectos:

10.1 Estrategia de Ubicación Física de las Áreas/Procesos/Negocios en caso de requerir continuidad de la operación en otra instalación.

Cada Área/Proceso/Negocio, el Comité de Contingencia y Continuidad ha definido las siguientes opciones de instalaciones para que cada Área/Proceso/Negocio traslade su operación con el fin de dar continuidad al servicio de esta.

SERVICIOS ALTERNOS ADICIONALES DISPONIBLES PARA EL PLAN DE RECUPERACIÓN	
Infraestructura	• Autopista Medellín Km 2,4 Costado Sur – Cota, Cundinamarca. Clic 80. • S3 Cra. 49a #40 # 86, Bogotá. • Sede Aut. Norte (Interconexión alterna demás sedes) Centro Empresarial El Prado Contacto: Maria Helena Vargas Teléfono: 6053131 ext 252
Backups	• Servidores alternos virtuales configurados en Data Center externo, con accesibilidad en línea a través de internet. • Servidores con respaldo externo y plan de continuidad de acuerdo con requisitos de Datacenter TIER III • Consola de Administración de Backups
Correo electrónico	• Servicio de correo en la nube.
Internet	• Canal principal- Une Epm • Canal alterno – S3
Telecomunicaciones	• Principal – Une • Alterno: • 1980 TIC • TeleOne
Servidores	• Servidores alternos físicos y/o virtuales configurados en Data Center externo, con accesibilidad en línea a través de internet. • Servidores con respaldo externo y plan de continuidad de acuerdo con requisitos de Datacenter TIER III
Pbx	Principal • PBXIP CooVox Alterno: • Vicidial
Ups	• Ups POWER SUN con Autonomía de 15 mm mientras se realiza el bypass con la planta eléctrica
Planta eléctrica	• La planta eléctrica es proporcionada por el Edificio Centro Empresarial El Prado.

10.2 Estructura Mínima para la operación en momentos de Contingencia

Cada Área/Proceso/Negocio de OIGAME CONSULTORES EMPRESARIALES SAS debe definir en la matriz de EMR, las necesidades básicas para instalar un porcentaje de su operación nuevamente

en el mismo lugar o en uno diferente, que garantice el servicio mínimo al cliente. Con esta información, se podrán gestionar los requerimientos necesarios con las áreas de infraestructura, tecnología, gestión humana, entre otras, para operar en contingencia.

Con base en los Reportes de Análisis de Impacto del Negocio por Servicios –BIA, los **Tiempos de Recuperación Objetivo (RTO),** son de máximo de 1 hora sin servicio.

La Estructura Mínima Requerida EMR para operar en momentos de contingencia, es la siguiente.

- Servicio de Internet
- Servicios de Telefonía – Dispositivo IP PBX ZYCOO y VICIDIAL
- Servidor Sistema de Administración de Cartera –SAC (BD SQL SERVER 2012 + IIS 8)
- Servidor de Base de Datos de Producción - (SQL Server 2012)
- Servidor de Aplicaciones IIS 8
- Servidor Base de Datos del Área de Datos-- (SQL Server 2012)
- Servidor de Archivos y FTPS –QNAP
- UTM Sophos, Firewall
- Servidor Controlador de Dominio
- Servidor de notificaciones – Mailing
- Servicios de respaldo
- Computadores de escritorio y portátiles

10.3 Escenarios de Riesgo y Estrategias de Contingencia para dar continuidad al servicio

Basados en los Riesgos identificados en el Análisis de Riesgos General de la empresa., cada área/proceso/negocio definirá en conjunto con el área de Continuidad, los riesgos que le afectan específicamente y las estrategias de contingencia específicas a aplicar para dar continuidad al servicio.

10.4 Tiempos Máximos Tolerables de Interrupción (MTPD) y Tiempos de Recuperación Objetivo (RTO)

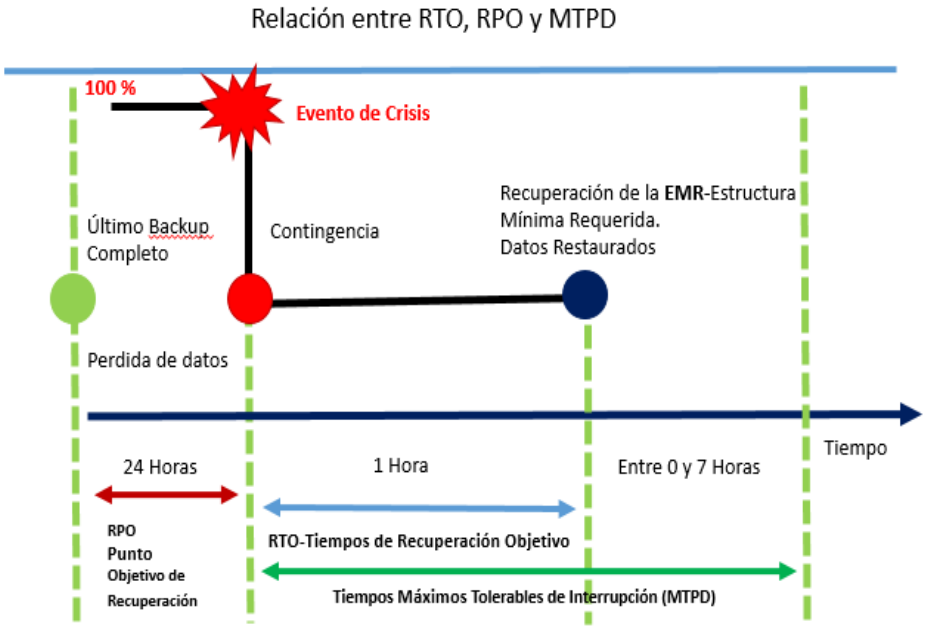
El Jefe de cada Área/Proceso/Negocio de OIGAME CONSULTORES EMPRESARIALES SAS debe definir los tiempos máximos de interrupción (MTPD), por proceso o por actividad, que significan el tiempo máximo durante el cual puede estar el servicio, proceso o actividad inoperante o detenida.

También debe definir el tiempo de recuperación objetivo (RTO) por proceso o actividad, que significa el tiempo en el cual se espera estar operando nuevamente al 100%.

En algunos casos, puede suceder que el MTPD sea igual al RTO, y que éstos ya estén convenidos contractualmente con los clientes.

Con esta información, se podrá avisar previamente al cliente interno o externo, cuál es el MTPD para que dicho cliente espere paciente este lapso de tiempo para continuar con la prestación del servicio.

Estos tiempos deben ser entregados por los Jefes de Área a los Responsables de la DE CONTINUIDAD DEL NEGOCIO, quien los consolidará para tenerlos en cuenta en pruebas y contingencias o emergencias reales.



Tiempos Máximos Tolerables de Interrupción (MTPD)

MTPD	0 y 7 Horas	<= 8 Horas	>8 ^ = < 12 Horas	>12 ^ = < 23 Horas
Recuperación de Internet	X			
Recuperación de Servicios de Telefonía	X			
Recuperación sistema de administración de cartera -SAC	X			
Recuperación servidor de base de datos de producción	X			
Recuperación servidor de aplicaciones IIS	X			
Recuperación servidor base de datos del área de datos	X			
Recuperación servidor de archivos y FTPS -QNAP	X			
Recuperación servidor de notificaciones - Mailing		X		
Recuperación servidor de documentos – Kawak	X			
Recuperación UTM Sophos, Firewall	X			
Recuperación servidor de Directorio Activo	X			
Recuperación consola de antivirus – Karpesky		X		
Recuperación servicios de correo – Office 365			X	

Recuperación servidor de cartera-SIIGO	X			
Recuperación firewall sede Administrativa- Sophos	X			

Tiempos de Recuperación Objetivo (RTO)

RTO	1 Hora	2 Horas	4 Horas
Recuperación de Internet	X		
Recuperación de Servicios de Telefonía	X		
Recuperación sistema de administración de cartera -SAC	X		
Recuperación servidor de base de datos de producción	X		
Recuperación servidor de aplicaciones IIS	X		
Recuperación servidor base de datos del área de datos	X		
Recuperación servidor de archivos y FTPS -QNAP		X	
Recuperación servidor de notificaciones - Mailing		X	
Recuperación servidor de documentos – Kawak			X
Recuperación UTM Sophos, Firewall	X		
Recuperación servidor de Directorio Activo	X		
Recuperación consola de antivirus – Karpesky		X	
Recuperación servicios de correo – Office 365			X
Recuperación servidor de cartera-SIIGO		X	
Recuperación firewall sede Administrativa- Sophos			X

11. PLAN DE CONTINGENCIA, CONTINUIDAD Y DRP ESPECÍFICO POR ÁREA, PROCESO O NEGOCIO

Basados en este PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO General, OIGAME CONSULTORES EMPRESARIALES SAS define específicamente para cada área, proceso o negocio un PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO específico compuesto por:

- Estructura Mínima Requerida para Operar en Contingencia
- Escenarios de Riesgo y Estrategias de Contingencia para dar Continuidad al Servicio
- Definición de MTPD y RTO
- Contactos en Momentos de Contingencia. En el cual se identifican las personas por parte de OIGAME CONSULTORES EMPRESARIALES SAS y del Cliente, con las cuales se debe establecer comunicación para declarar el estado de contingencia e informar posteriormente el cierre de la misma.

En el administrador de documentos de OIGAME CONSULTORES EMPRESARIALES SAS, /Continuidad del Negocio /Plan de Contingencia y Continuidad/ Planes de CCN específicos por Área/Proceso/Negocio se visualizan los PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO específicos por cada área, proceso o negocio, los cuales han sido estructurados y validados entre el área de Continuidad y los Líderes de dichas áreas, procesos, negocios.

12. PLAN DE RETORNO A LA OPERACIÓN NORMAL

Para retornar a la operación normal, OIGAME CONSULTORES EMPRESARIALES SAS desde cualquiera de sus áreas seguirá los siguientes parámetros:

12.1 Recuperación Tecnológica

Los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) contactarán al área de Tecnología de OIGAME CONSULTORES EMPRESARIALES SAS y de su cliente cuando aplique, haciendo los requerimientos necesarios de reinstalación y/o configuración de la infraestructura tecnológica del área afectada.

Esta recuperación tecnológica además tendrá en cuenta los parámetros establecidos en el Plan de Contingencia Tecnológico.

12.2 Recuperación Operativa

Los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes), teniendo en cuenta su conocimiento sobre la operación que lideran, deberán reasignar las responsabilidades y coordinar a sus funcionarios y recursos para retomar el cumplimiento de la labor o servicio al 100%.

12.3 Recuperación de Documentos/Archivos

En caso de presentarse deterioro o daño de Documentos/Archivos debido a la emergencia o contingencia, los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) tendrán en cuenta las siguientes recomendaciones. Si resultado de estos tratamientos, hay documentos/archivos que no pueden ser recuperados, se consultará con el los Responsables DE CONTINUIDAD DEL NEGOCIO para validar y llevar a cabo el procedimiento de eliminación o borrado seguro de la información, teniendo en cuenta el aviso a los clientes sobre la información afectada por la emergencia/contingencia.

12.4 Procedimiento de tratamiento y recuperación de documentos físicos afectados por un incidente (documentos sueltos, en carpetas, en AZs, en cajas, etc.)

Cuando los documentos físicos son afectados por un incidente como inundación o incendio se debe actuar así:

INUNDACIÓN o MOJADO

- Separar el material afectado para evaluar y cuantificar el estado del mismo.
- Aquel material que se detecte con posibilidad de recuperación se debe separar en un espacio libre y amplio donde pueda extenderse para su secado.
- Posterior al secado, separar el material que realmente se recuperó del material que según la valoración física perdió su información debido al secado.
- Cuantificar la magnitud del daño, para tomar acciones sobre información a los Clientes y Reclamación de Pólizas.
- Identificar y decidir qué acción de conservación o eliminación se tomará con el material afectado, luego de recuperar su información.

INCENDIO

- Separar el material afectado para evaluar y cuantificar el estado del mismo.
- Realizar una valoración del material para identificar cuál es recuperable y cuál no. El material recuperable es aquel al cual se le puede extraer la información que contenía inicialmente.
- Cuantificar la magnitud del daño, para tomar acciones sobre información a los Clientes y Reclamación de Pólizas.
- Identificar y decidir qué acción de conservación o eliminación se tomará con el material afectado, luego de recuperar o no su información.

12.5 Procedimiento de tratamiento y recuperación de medios magnéticos afectados por un incidente (Cds, Cintas, Rollos de microfilm, Cartridges, Videos, Tapes backup)

INUNDACIÓN o MOJADO

- Separar el material afectado para evaluar y cuantificar el estado del mismo.
- Realizar un secado del material afectado.
- Hacer una revisión total del material en los medios de lectura necesarios, para identificar si la información e imágenes contenidas en ellos se conserva intacta o tuvo alteraciones debido al incidente.
- Separar el material que realmente se puede conservar del material que según la valoración física perdió su información.
- Cuantificar la magnitud del daño, para tomar acciones sobre información a los Clientes y Reclamación de Pólizas.
- Identificar y decidir qué acción de conservación o eliminación se tomará con el material afectado, luego de recuperar o no su información.

INCENDIO

- Separar el material afectado para evaluar y cuantificar el estado del mismo.
- Hacer una revisión total del material en los medios de lectura necesarios, para identificar si la información e imágenes contenidas en ellos se conserva intacta o tuvo alteraciones debido al incidente.
- Realizar una valoración del material para identificar cuál es recuperable y cuál no. El material recuperable es aquel al cual se le puede extraer la información que contenía inicialmente.
- Cuantificar la magnitud del daño, para tomar acciones sobre información a los Clientes y Reclamación de Pólizas.
- Identificar y decidir qué acción de conservación o eliminación se tomará con el material afectado, luego de recuperar su información.

13. RETROALIMENTACIÓN

Superada la situación de emergencia/contingencia, el(as) área(s) de OIGAME CONSULTORES EMPRESARIALES SAS debe realizar los siguientes análisis para retroalimentarse sobre lo ocurrido, lo cual será coordinado por el área de Continuidad:

13.1 Análisis y Evaluación del Incidente

Paralelo al retorno normal de la operación (numeral 13 del PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO) los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, , Líderes) deberán evaluar la magnitud del daño que se ha producido determinando:

1. Recurso Humano afectado
2. Infraestructura Física afectada
3. Sistemas afectados

Para la realización de este reporte, se tendrá en cuenta un formato de retroalimentación sobre la emergencia/contingencia, el cual deberá desarrollar y aprobar el proceso de SIG, y debe ser entregado a los Responsables DE CONTINUIDAD DEL NEGOCIO para llevarlo a Comité de Contingencia y Continuidad.

13.2 Análisis de Pérdidas de Información

Los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) deberán determinar qué información se vio afectada con la emergencia/contingencia.

Para la realización de este reporte, se tendrá en cuenta un formato de retroalimentación sobre la emergencia/contingencia, el cual deberá desarrollar y aprobar el proceso de SIG, y debe ser entregado a los Responsables DE LA CONTINUIDAD DEL NEGOCIO para llevarlo a Comité de Contingencia y Continuidad.

13.3 Evaluación de Resultados

Con la información de los reportes, los Responsables de la CONTINUIDAD DEL NEGOCIO convocará al Comité de Contingencia y Continuidad e invitará a los CIEC (si aplica por Emergencia), para evaluar la magnitud de la Emergencia/Contingencia y definir los planes de acción a seguir con el fin de prevenir nuevas situaciones o corregir aquellas afectaciones que aún no han sido subsanadas.

14. PLAN DE PRUEBAS DEL PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO

Anualmente se realizará una (1) prueba de contingencia operativa de OIGAME CONSULTORES EMPRESARIALES SAS con el fin de evaluar la capacidad de reacción del personal e infraestructura física y tecnológica, además de probar la eficiencia del PLAN DE CONTINGENCIA PARA LA CONTINUIDAD Y DRP DEL NEGOCIO. Estas pruebas pueden involucrar o nó al cliente, según se defina con cada Área/Proceso/Negocio.

Adicionalmente se realizarán las pruebas que sean solicitadas directamente por el cliente para evaluar situaciones de emergencia/contingencia específica.

El área de Tecnología de OIGAME CONSULTORES EMPRESARIALES SAS también realizará anualmente pruebas a toda la infraestructura tecnológica de la compañía, según lo describen en el Plan de Contingencia y Continuidad Tecnológico del numeral 12.

Los Responsables de la CONTINUIDAD DEL NEGOCIO se encargará de coordinar con los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) las fechas de pruebas para generar un cronograma que deberá ser llevado a cabo puntualmente.

15. PLAN DE CONTINGENCIA EN CASO DE OCURRENCIA DE EVENTOS O DESASTRES EN LAS INSTALACIONES DEL CLIENTE DONDE OPERA OIGAME CONSULTORES EMPRESARIALES SAS

En caso de presentarse una contingencia en las instalaciones del cliente donde operamos, es importante que OIGAME CONSULTORES EMPRESARIALES SAS esté enterado de su Plan de Contingencia y Continuidad del Negocio, y de la protección que brindarán al personal de OIGAME CONSULTORES EMPRESARIALES SAS

Es responsabilidad del cliente contar con un plan de contingencia para estos casos. Los Jefes de Área (Gerentes, Directores, Coordinadores, Supervisores, Líderes) de los Procesos/Negocios que operan en instalaciones del cliente, son responsables de averiguar con este último cuál es el plan de contingencia a seguir y divulgarlo entre los funcionarios correspondientes.

16. PÓLIZAS

Adicional a las Estrategias de Contingencia descritas en el presente documento, OIGAME CONSULTORES EMPRESARIALES SAS cuenta con Pólizas que soportan todo su negocio así:

TIPO POLIZA	ASEGURADORA O AGENCIA	AMPARO	COBERTURA
TODO RIESGO DAÑO MATERIAL **RESPONSABILIDAD CIVIL EXTRACONTRACTUAL**	Sura Nro. 0744422-8	Extracontractual	- Responsabilidad civil predios, labores y operaciones. - Responsabilidad civil gastos médicos de urgencia - Responsabilidad civil empleador - Responsabilidad civil gastos de defensa -Responsabilidad civil manejo indebido de datos personales - Transporte vehículos propios - Fuga de información de terceros - Software malicioso o virus informático - Comunicación fraudulenta
		Fraude de empleados	- Básico fraude de empleados - Fraude de empleados no identificados - Estafa - Abuso de confianza - Hurto simple - Falsedad de documentos
		Protección legal	- Asistencia legal - Defensa legal

		Datos de los clausulados	- Responsabilidad civil Daños a terceros - Protección Digital - Protección Legal - Fraude de Empleados
		Daños materiales	- Daños materiales a contenidos - Daños materiales equipos de computo - Terremoto contenidos - Terremoto equipos de computo - Daño interno equipos de cómputo y procesamiento
		Asistencia	- Asistencia integral
		Sustracción	- Violencia a contenidos - Violencia equipos de computo

17. ANEXOS

17.1 Personas con Disponibilidad para Fines de Semana

- Operaciones: María Helena Vargas
- Administrativa: Jorge Iván Vargas

Que por control de llaves y accesos se rotarían Mensualmente con:

- Operaciones: Alexander Vargas
- Administrativa: Marcela Díaz

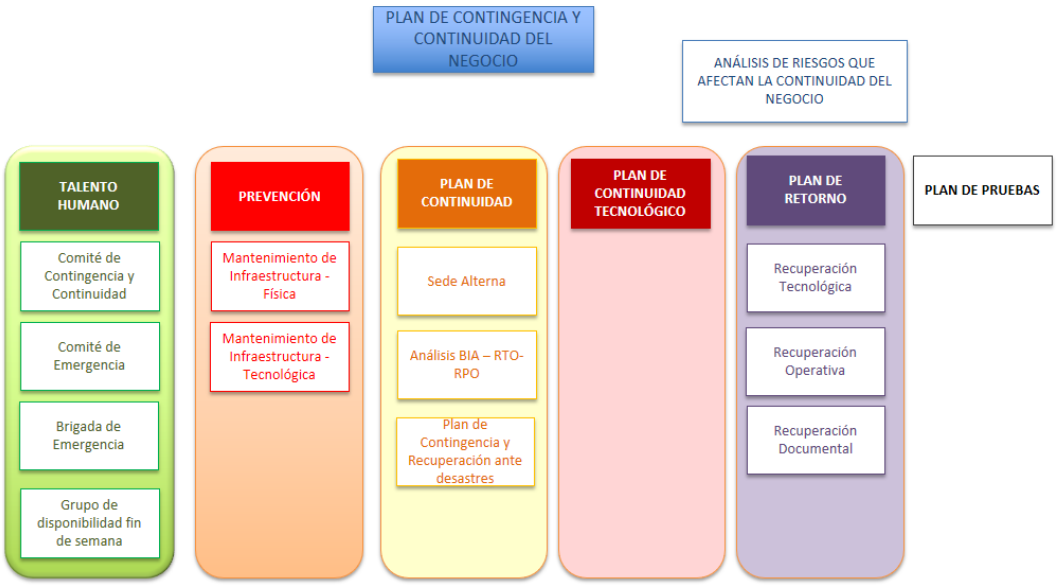
17.2 Listado de Proveedores a Contactar en Momentos de Contingencia

- UNE EPM Comunicaciones
  Jose Moreno 6065555 Ext. 5109 Cel. 304233392
- 1980 TIC
  Soporte 4430419 Julian Morales Cel. 3163550795
- TELEONE
  Servicio al Cliente 5938777 Maria Rojas
- GMS
  Servicio al cliente 7443993
  S3
  Servicio al Cliente 6510051 Luz Avila
- RentaSitemas
  Servicio al Cliente6554505 Mauricio Gutierrez
- KAWAK, 3906364
  Servicio al cliente
- SIIGO
  Atenciòn al cliente 6337150

- IT-OUTSOURCING
  Servicio al cliente 7431700
- INDENOVA
  Servicio al cliente 3099320
- SAC
  Mesa de servicio Mantis

18. MAPA CONCEPTUAL

6 Mapa Conceptual PCCN –



19. CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Modificación
1	10/11/2015	Documento Inicial
2	11/10/2016	Se modifica de acuerdo con la nueva estructuración de la compañía.

3	12/03/18	Se realizan las modificaciones solicitadas en el pasado comité de seguridad de la información realizado el 14/02/2018, acta 001: • Modificar Oigame Consultores Empresariales Ltda por Oigame Consultores Empresariales SAS. • Modificar den el punto 10.1 Infraestructura las direcciones de las sedes disponibles. • El canal alterno actualmente es S3. • El nuevo operador de telecomunicaciones es Teleamigo. • Con el cambio de sede la planta eléctrica es proporcionada por el edificio, Centro empresarial El Prado. • La póliza actual Todo Riesgo se contrató con la compañía Sura Seguros, se deben modificó los amparos y coberturas correspondientes. • En el punto 17 Anexos modificar el nombre del responsable del control de llaves y accesos para administrativa por: Marcela Diaz.
4	22/01/2020	Se realiza la inclusión del plan DRP y se establece que se ejecutará de forma anual de acuerdo con lo requerido por la compañía y sus clientes, adicionalmente se modifica los proveedores de contingencia y sus números de contacto. Para el equipo de contingencia y su distribución no es necesario que sea de forma presencial. Cambio de Líder de Continuidad del Negocio a Responsables de la Continuidad del Negocio. Se cambia proveedor de comunicaciones Teleamigo a TeleOne. Se realiza la actualización e identificación de los activos críticos de la compañía.