1. OBJETIVO

Coordinar el desarrollo de los procesos que garanticen la continuidad de las actividades de la Compañía.

2. ALCANCE

Aplica para todo el personal ubicado en las diferentes sedes de la compañía y las que llegaren a inaugurarse o asumirse, desde el momento de la declaración de una contingencia de riesgo ALTO, hasta la implementación y operación desde la sede o sedes alternas de contingencia.

3. RESPONSABILIDADES

Es responsabilidad del Representante del SIG coordinar los procesos de administración de la continuidad de la operación de los sistemas de tratamiento de información de la Compañía frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- ✓ Identificar y priorizar los procesos críticos de las actividades de la Compañía.
- ✓ Asegurar que todos los integrantes de la Compañía comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la Compañía.
- ✓ Elaborar y documentar una estrategia de continuidad de las actividades de la Compañía consecuente con los objetivos y prioridades acordados.
- ✓ Proponer planes de continuidad de las actividades de la Compañía de conformidad con la estrategia de continuidad acordada.
- ✓ Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- ✓ Coordinar actualizaciones periódicas de los planes y procesos implementados.
- ✓ Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la compañía.
- ✓ Proponer las modificaciones a los planes de contingencia.

4. CONTINUIDAD DE LAS ACTIVIDADES Y ANÁLISIS DE LOS IMPACTOS

Con el fin de establecer un Plan de Continuidad de las Actividades de la Compañía se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.

- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

"Documento Privado para uso interno – Prohibida su Reproducción Parcial o Total sin Previa Autorización"

- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

5. ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE CONTINUIDAD DE LAS ACTIVIDADES DE LA COMPAÑÍA

Los propietarios de procesos y recursos de información, con la asistencia del Líder del SGI y el Oficial de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Compañía.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
d) Documentar los procedimientos y procesos acordados.
e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

1. Objetivo del plan.
2. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
3. Procedimientos de divulgación.
4. Requisitos de la seguridad.
5. Procesos específicos para el personal involucrado.
6. Responsabilidades individuales.
7. Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades de la Compañía requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

6. MARCO PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DE LA COMPAÑIA

Se mantendrá un solo marco para los planes de continuidad de las actividades de la Compañía a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades de la Compañía se tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la Compañía y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.

c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la compañía o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la Compañía.

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.

g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

7. MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DE LA COMPAÑIA.

Debido a que los planes de continuidad de las actividades de la Compañía pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Representante del SIG establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado al representante de la Gerencia o del SIG. Se deberán utilizar diversas

técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas deben incluir preferiblemente:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).

c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).

d) Realizar ensayos completos probando que el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la compañía deben tener en cuenta preferiblemente los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de la Compañía en paralelo, con operaciones de recuperación fuera del sitio principal).

b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos adquiridos).

Los planes de continuidad de las actividades de la Compañía serán revisados y actualizados periódicamente, para garantizar su eficacia permanente.

8. POLÍTICAS ESPECÍFICAS

8.1.1. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.

OIGAME CONSULTORES EMPRESARIALES S.A.S., debe asegurar la identificación e implementación de actividades y procedimientos que permitan garantizar la continuidad de sus funciones e información crítica, ante un evento de desastre o una interrupción mayor, sin disminuir los niveles de seguridad establecidos.

Esto debe ser independiente tanto del medio tecnológico que utilice OIGAME CONSULTORES EMPRESARIALES S.A.S. como de la posibilidad de que la información se dañe, se destruya o no esté disponible por una extensión de tiempo.

8.1.2. INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

- ✓ Se debe desarrollar y mantener un proceso y/o procedimiento de gestión para la continuidad de negocio, el cual debe incluir controles para identificar y reducir las consecuencias de un evento de desastre o interrupción mayor, además del proceso de valoración de riesgos, limitar las consecuencias de las interrupciones con el fin de garantizar la disponibilidad de la información requerida para los procesos críticos de negocio.

- ✓ Todos los sistemas de información que soportan las funciones críticas necesarias para que OIGAME CONSULTORES EMPRESARIALES S.A.S. realice sus negocios, deben tener un Plan de Recuperación de Tecnología que le permitan garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupción mayor, los cuales deben ser probados, previo a su puesta en producción.

- ✓ La gestión para la continuidad de negocio de OIGAME CONSULTORES EMPRESARIALES S.A.S., debe cubrir los requerimientos mínimos de seguridad de la información necesarios en la continuidad de los procesos críticos.

8.1.3. CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS.

- ✓ Las evaluaciones de riesgo para continuidad de negocio se deben efectuar con plena participación de los dueños de los activos y procesos de negocio, vinculando en conjunto todos los aspectos del riesgo con el fin de tener un panorama completo de los requerimientos de continuidad de negocio de OIGAME CONSULTORES EMPRESARIALES S.A.S.

- ✓ En el análisis de riesgos se deben identificar los eventos que pueden ocasionar interrupciones en los procesos de OIGAME CONSULTORES EMPRESARIALES S.A.S., la probabilidad de ocurrencia, el impacto en la función misional de la organización y las consecuencias en seguridad de la información.

- ✓ Se debe desarrollar una estrategia de continuidad de negocio, considerando los resultados de los análisis de riesgo e impacto al negocio para determinar el enfoque global para la continuidad de negocio. Además, se debe crear un plan para la implementación de esta estrategia.

- ✓ Los gestores del Plan de Continuidad de Negocio deben actualizar el análisis de riesgos, impacto al negocio y estrategias de continuidad al menos una vez al año o cuando haya cambios significativos en los procesos de OIGAME CONSULTORES EMPRESARIALES S.A.S., para asegurar que éstos continúan reflejando las necesidades de la organización en cuanto a continuidad del negocio.

8.1.4. DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD QUE INCLUYAN LA SEGURIDAD DE LA INFORMACIÓN.

El Plan de Continuidad de Negocio de OIGAME CONSULTORES EMPRESARIALES S.A.S y evaluación de riesgos debe contemplar:

- ✓ La identificación de Tiempos de Recuperación Objetivos (RTO) para con activos críticos de OIGAME CONSULTORES EMPRESARIALES S.A.S que, por su importancia en el cumplimiento de objetivos misionales de la Organización, requieren ser restablecidos en el menor tiempo posible.

- ✓ La identificación de Puntos de Recuperación Objetivos (RPO) o datos mínimos requeridos para recuperar la operación básica de activos críticos de OIGAME CONSULTORES EMPRESARIALES S.A.S.

- ✓ La identificación de análisis de impactos del Negocio a la Empresa (BIA).

- ✓ La identificación de responsabilidades y procedimientos adecuados para gestionar actividades de Continuidad de Negocio con mínimos niveles de seguridad de la información requeridos por OIGAME CONSULTORES EMPRESARIALES S.A.S.

- ✓ El apoyo de los gestores de Continuidad de negocio de OIGAME CONSULTORES EMPRESARIALES S.A.S para integrar en los esquemas de comunicaciones requeridos para la activación del plan de Continuidad de Negocio en las distintas áreas y funcionarios involucrados en los procesos críticos de OIGAME CONSULTORES EMPRESARIALES S.A.S.

- ✓ Las actividades y procedimientos establecidos deben contar con un programa de pruebas y simulacros para la validación y mejora continua de Plan de contingencia de OIGAME CONSULTORES EMPRESARIALES S.A.S.

8.1.5. ESTRUCTURA PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DE NEGOCIO.

La estructura metodológica que adopta OIGAME CONSULTORES EMPRESARIALES S.A.S para la planificación de las acciones en la creación del plan de Continuidad de Negocio debe contemplar actividades como:

- ✓ Identificación de procesos críticos de negocio.

- ✓ Análisis de los riesgos de no disponibilidad.

- ✓ Análisis del impacto.

- ✓ Identificación e implementación de las estrategias de recuperación.

- ✓ Definición de las actividades para atender una emergencia.

- ✓ Definición de las actividades para mantener operativos los planes de continuidad de negocio.

- ✓ Definición, implementación y monitoreo de la ejecución de programas de capacitación y sensibilización sobre continuidad de negocio.

8.1.6. PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO.

- ✓ El Plan de Continuidad de Negocios, planes de contingencia y reparación de equipos deben ser sometidos a pruebas y revisiones periódicas con el fin de asegurar que son relevantes, efectivos, prácticos y factibles.

- ✓ Las pruebas del Plan de Continuidad del Negocio deben asegurar que todo el personal que participa en el equipo de recuperación y otro personal pertinente, como funcionarios, contratistas

y clientes son conscientes de los planes, de sus funciones y responsabilidades cuando se ejecuta un plan.

- ✓ Las pruebas para los Planes de Continuidad de Negocio deben ser programadas, la programación de las pruebas debería indicar cómo y cuándo se va a probar cada elemento del plan; cada uno de los elementos se debería probar con frecuencia.

- ✓ Los resultados de las pruebas deben ser documentados adecuadamente y cada prueba debe ser revisada para establecer las oportunidades de mejoramiento que permitirán mantener y reevaluar el plan.

- ✓ Los Planes de Continuidad de Negocio son probados al menos una vez al año o cuando se presenten cambios relevantes en los procesos críticos de OIGAME CONSULTORES EMPRESARIALES S.A.S y deben tener definidas e implementadas actividades de actualización y mantenimiento.

8.1.7. PERIODICIDAD REVISIÓN POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Se establece en OIGAME CONSULTORES EMPRESARIALES S.A.S que la periodicidad de revisión de la política de continuidad del negocio será anual y la misma se llevará a cabo en el Comité de Seguridad de la Información propuesto.

9. CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Modificación
1	15/06/2013	Documento Inicial
2	10/11/2015	Se Modifica de acuerdo con la nueva estructura documental de la compañía
3	10/11/2017	Se realiza el cambio en el nombre del documento que estaba en singular "Política" por su plural "Políticas". Se incluyen los siguientes numerales: 8. POLÍTICAS ESPECÍFICAS 8.1.1. Aspectos de seguridad de la información en la gestión de la continuidad de negocio.

		8.1.2. Inclusión de la seguridad de la información en la gestión de la continuidad del negocio. 8.1.3. Continuidad del negocio y evaluación de riesgos. 8.1.4. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información. 8.1.5. Estructura para la planificación de la continuidad de negocio. 8.1.6. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.
4	12/03/2018	Se incluye la política 8.1.7 Periodicidad revisión política de continuidad del negocio, según el pasado comité de Seguridad de la Información realizado el 14/02/2018.