1. OBJETIVO Y ALCANCE

Establecer las políticas y procedimiento que regulan la prevención del riesgo y la definición de Planes de Contingencia, a fin de prever la perdida de archivos e información relevante del negocio frente a un siniestro o eventualidad no deseada, garantizando la continuidad de las operaciones de la empresa.

2. APLICABILIDAD

Estas políticas y procedimiento aplican desde la identificación de riesgos y definición de planes de contingencia, hasta el resguardo de la información de la empresa y la implementación de los planes de contingencia definidos para la continuidad de las operaciones de la empresa.

3. RESPONSABILIDAD

- El Director Financiero es responsable de la aprobación y supervisión de estas políticas y procedimiento.
- El Gerente Administrativo y de Cumplimiento es responsable de la implementación, control y actualización de estas políticas y procedimiento.
- El Encargado de Tecnología es el responsable de la ejecución de estas políticas y procedimiento.

4. POLÍTICAS

4.1 Anualmente el Área de Tecnología debe realizar análisis de riesgos informáticos que permitan identificar y actualizar la política y las acciones para impedir eventos que puedan interrumpir la continuidad de las operaciones del negocio.

4.1.1 Un Plan de Continuidad del Negocio inicia con un análisis de riesgos el cual permita identificar los riesgos existentes que podrían impedir la continuidad del negocio.

4.1.2 El análisis de riesgos incluye la identificación de amenazas como:

- **Desastres Naturales:** fuego, pérdida de la infraestructura o de los servicios críticos tales como: agua, comunicaciones y energía.
- **Desastres causados por el hombre:** daños deliberados o accidentales al equipo o a los datos principales, huelgas o interrupciones del trabajo.
- **Fallas en los sistemas:** aberturas o brechas de seguridad, acceso deliberado o accidental a la

información confidencial o propietaria.

4.1.3 El plan de Continuidad del Negocio define claramente los Tiempos Objetivos de Recuperación (RTO) y los Puntos Objetivos de Recuperación (RPO).

4.1.4 Deberá conformarse el Comité Ejecutivo de Continuidad del Negocio, conformado por los líderes de cada área crítica de la empresa. (Finanzas-Gerencia Administrativa y Cumplimiento, logística, TI)

4.1.5 El Comité de Continuidad del Negocio debe participar en todas las reuniones oficiales correspondientes al Plan de Continuidad del Negocio para conocer la metodología de Planes de Acción.

4.1.6 El Comité de Continuidad del Negocio es el responsable de capacitar a todo el personal de las áreas críticas de la empresa en la metodología a utilizar.

4.1.7 El Comité de Continuidad del Negocio garantiza la realización de las pruebas y actualizaciones del Plan de Continuidad del Negocio por parte de los responsables de cada área crítica de la empresa.

4.1.8 El Comité de Continuidad del Negocio tiene un marco estándar para todos los planes de la continuidad del negocio. De igual manera, publica y comunica a los dueños de los planes de continuidad del negocio el formato a utilizar para su documentación.

4.2 MARCO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

4.2.1 El Plan de Continuidad del Negocio considera los siguientes aspectos:

- Es desarrollado dentro de un marco metodológico, el cual garantice su funcionalidad y efectividad.
- Tiene un plan de mantenimiento y prueba.
- Es probado por lo menos una vez al año de manera total.
- Contempla los entrenamientos, horarios y requisitos de educación para todo el personal involucrado.

4.2.2 El Plan de Continuidad del Negocio debe ser aprobado por el Comité Ejecutivo de Continuidad del Negocio antes de su desarrollo e implementación y contener toda la documentación necesaria, debidamente aprobada por los Encargados de las áreas críticas de la empresa.

4.2.3 El Plan de Continuidad del Negocio debe contemplar todos los requisitos necesarios para garantizar su recuperación, según lo determinado por el Comité de Continuidad del Negocio.

4.3 Desarrollo y Ejecución del Plan de Continuidad del Negocio incluyendo la Seguridad de la

Información.

4.3.1 El Plan de Continuidad del Negocio contempla toda la información confidencial y no confidencial necesaria por cada área crítica de la empresa, la cual, es desarrollada bajo un esquema de acciones y procedimientos, que permite a la empresa su recuperación ante un evento catastrófico y/o inesperado.

4.3.2 El Plan de Continuidad del Negocio se debe proteger y considerar como información confidencial.

4.3.3 Los planes se deben almacenar apropiadamente, manteniendo una copia en las instalaciones del sitio primario y una copia en las instalaciones del sitio alterno.

4.3.4 Todos los Planes de la Continuidad del Negocio deben restaurar, recuperar y mantener las operaciones de la empresa en el tiempo estipulado y establecido.

4.3.5 El Comité de Continuidad del Negocio debe asegurar que todas las copias del Plan de Continuidad del Negocio sean actualizadas y distribuidas de manera apropiada.

4.4 Manejo del Documento del Plan de Continuidad del Negocio

4.4.1 El Comité de Continuidad del Negocio de la empresa debe establecer los procedimientos para manejar y mantener en todas partes el documento del Plan de Continuidad del Negocio, para minimizar los riesgos de seguridad en el manejo de la información y cumplir con los requerimientos y normativas.

4.5 Prueba, Mantenimiento y Actualización del Plan de Continuidad del Negocio

4.5.1 Los Planes de Continuidad del Negocio deben mantenerse en constante actualización y ejecución. De esta manera, se garantizará la funcionalidad y efectividad del Plan de Continuidad del Negocio ante cualquier interrupción inesperada.

4.5.2 Todos los Planes de Continuidad del Negocio tienen un calendario de mantenimiento y prueba. (Ver Plan de Mantenimiento y Prueba)

4.5.3 Los Planes de Continuidad del Negocio que soportan las áreas más críticas deben ser probados por lo menos una vez cada seis meses.

4.5.4 El proceso de la prueba debe ser determinado por el Comité de Continuidad del Negocio y aprobado por el Comité Ejecutivo.

4.5.5 Los Planes de Continuidad del Negocio serán corregidos y probados de presentarse cambios significativos en la empresa. Las pruebas deben ser documentadas y los resultados de estas deben ser divulgados a los dueños de cada área crítica de la empresa, que forme parte del plan.

4.5.6 El Plan de Continuidad del Negocio incluye el desarrollo de los criterios para la ejecución, mantenimiento, prueba, requisitos necesarios y la determinación del estado del plan para su activación.

4.5.7 Los responsables de cada área crítica de la empresa que forman parte del Plan de Continuidad del Negocio tienen la obligación de coordinar todas las actualizaciones del plan correspondiente a su área, integrando la documentación y actualización de

aspectos legales.

4.6 Cumplimiento

4.6.1 El Plan de Continuidad del Negocio se debe cumplir de acuerdo con los procesos definidos por el Comité de Continuidad del Negocio.

4.6.2 Los responsables de cada área crítica de la empresa con su equipo de recuperación que forman parte del Plan de Continuidad del Negocio tienen la obligación de cumplir con los tiempos y procedimientos establecidos en el manual de continuidad del negocio para garantizar la recuperación de sus procesos.

4.7 RIESGOS INTERNOS Y EXTERNOS

Internos:

1) Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción. - (R1). Riesgo interno que tiene baja probabilidad de ocurrencia y consiste en el robo, alteración o extracción de la información que es considerada confidencial o clasificada como reservada por deficiencia en las políticas de seguridad o Configuración ineficiente del cortafuego de la entidad. Al materializarse, el impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional. Tipo de riesgo: Tecnología.

2) Falla técnica en equipos servidores, de escritorio o de comunicaciones. - (R2). Riesgo interno que corresponde al daño físico o lógico de un equipo servidor, de escritorio o de comunicaciones que afecta el funcionamiento de un sistema de información crítico o de servicio por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los usuarios que hace que el servicio quede inoperante o Inestable. Tipo de riesgo: Tecnológico.

3) Falla técnica en sistemas de información - (R3). Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación o incompatibilidad entre software que afectan a los sistemas de información que genera Inoperancia o inestabilidad de los sistemas de información. Tipo de riesgo: Tecnológico.

4) Ausencia de personal de la Dirección de Tecnologías de la Información y las Comunicaciones que brindan soporte y mantenimiento a los a los sistemas de información. - (R4). Riesgo interno. Corresponde a la falta o inasistencia en un momento dado, de un ingeniero o técnico de la Dirección de TIC que realiza actividades de soporte a usuarios o de administración técnica sobre un sistema de información crítico de la Empresa por enfermedad, muerte o incapacidad de los funcionarios responsable o demoras en la asignación de funcionarios a la Dirección de TIC, lo que genera inoperancia o inestabilidad de los sistemas de información. Tipo de Riesgo: Operativo. PLAN DE CONTINGENCIAS.

5) Mal uso de hardware y/o software por parte de los USUARIOS - (R5). Riesgo interno. Consiste en el riesgo que corre la EMPRESA por un uso inadecuado de los equipos de cómputo, software y/o

sistemas de información por parte de los funcionarios por deficiencias en el conocimiento y uso de las herramientas tecnológicas o por uso mal intencionado de los mismos lo que puede dejar generar interrupción del funcionamiento de los equipos donde se alojan los sistemas de información críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

6) Calentamiento del centro de cómputo - (R6). Riesgo interno que consiste en el aumento de temperatura dentro del centro de cómputo y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, de comunicaciones y telefónicos dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos. Tipo de riesgo: Tecnología

Externos:

7) Caída o interrupción del sistema eléctrico - (R7). Riesgo externo. Corresponde al corte del servicio de energía eléctrica en la Contraloría de Bogotá por parte de falla externa en el proveedor del servicio, corte eléctrico que genera interrupción del funcionamiento de los equipos donde se alojan los aplicativos críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

8) Caída del canal de internet - (R8). Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet en la Empresa, lo que ocasionaría suspensión de los servicios de correo y de los aplicativos críticos de la entidad. Tipo de riesgo: Tecnológico.

9) Caída del Servicio Telefónico - (R9). Riesgo externo correspondiente a la suspensión del servicio por daños o fallas PLAN DE CONTINGENCIAS DE TI que de presentarse genera la ausencia de comunicación telefónica en la entidad. Tipo de riesgo: Tecnológico.

10) Caída de servicios por virus informático - (R10). Riesgo externo. Es el riesgo de infección de los equipos servidores y de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia o inestabilidad de los sistemas. Tipo de riesgo: Tecnológico.

11) Suspensión del servicio por sismo, inundación o incendio - (R11). Riesgo externo. Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo, inundación o incendio que afecte la infraestructura tecnológica de los sistemas de información críticos de la empresa generando suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia de los sistemas o inestabilidad de estos. Tipo de riesgo: Operativo.

5. PROCEDIMIENTO

RESPONSABLE	ACTIVIDADES	FORMULARIOS/ HERRAMIENTAS

Encargado de Tecnología	En caso de Desastres Naturales (R11):
	• Verificar el estado físico de los equipos y si están hábiles para el funcionamiento. (30 Minutos)
	• En caso de que estén hábiles verificar si las aplicaciones están funcionando de manera correcta y hacer pruebas (1h).
	• En caso de que no estén funcionando los equipos configurar el servidor de contingencias para su uso en locación externa Descargando de la Nube (DropBox) la última copia de Bases de Datos (3 horas)
	• Redireccionar todos los accesos al Servidor de contingencias (2horas)
	• Realizar pruebas de conectividad y aplicaciones activas (1 hora).
	
	En caso de Interrupción del Sistema Eléctrico (R7):
	• Verificar el tipo de avería teniendo en cuenta:
	  • Avería de fuente primaria (Empresa externa suplidora de energía): Pasar a fuentes alternativas como planta eléctrica, ups y/o inversor. Estimar el tiempo de duración de las fuentes alternativas y realizar respaldos de seguridad de todos los medios y sistemas tanto internos como externos. (4horas)
	  • Avería fuente Alternativa de energía (Planta o UPS): pasar a fuente primaria y evaluar reparación o cambio de fuente alternativa. Realizar copia de seguridad de todos los medios y sistemas tanto internos como externos. (4 horas)
	
	En caso de Caída Servicio Telefónico (R9):
	
	• Verificar tipo de avería contactando a la empresa suplidora y estimar tiempo de solución.
	• Utilizar medios telefónicos celulares y correos electrónicos para facilitar la comunicación. (2horas)
	
	En caso Caída del Servicio de Internet (R8):	

	• Verificar tipo de avería contactando a la empresa suplidora y estimar tiempo de solución. • Utilizar internet de contingencias (Altice Dominicana) y configurar para tener accesos a la red principal de la empresa. (2horas**)**	
Encargado de Tecnología	En caso de Fallas en los Sistemas (R3): • Se procede a identificar el tipo de falla en los Sistemas verificando: ✓ Falla en los Sistemas Operativos de los Servidores: Se procede a restaurar la última imagen de las Máquinas Virtuales colocada en los servidores (2Horas) ✓ Falla del ERP**:** Se procede a verificar si es un problema de Bases de datos o de la Aplicación. Si es de la Aplicación se redirecciona el acceso al servidor de contingencias y se verifica la conectividad de los usuarios (2 horas). ✓ En caso de ser un problema de Base de Datos se Restaura la última copia de seguridad de y se realiza la prueba de conectividad. (1 hora)	
Encargado de Tecnología	Desastres causados por el hombre (R1, R2, R3, R4, R5, R6): • Identificar el tipo de daño provocado: ✓ Robo de Servidor: Proceder a redireccionar los accesos a servidor de Contingencias y verificar conectividad. Cotizar nuevo servidor para su inmediata compra. 4 horas. ✓ En caso de ataque a la seguridad: Verificar puerto de acceso y log de entrada a los Routers. Correr los antivirus y cambiar todas las contraseñas de los usuarios a una temporal. Verificar el tipo de datos extraídos y contactar posibles afectados en dichos documentos par información. Abrir caso en la oficialía de delitos tecnológicos para investigación. Inhabilitar cuenta de usuario utilizada para el acceso no autorizado en caso de ser confirmada. (8 horas)	

Revisado por: _ERICKSON CASTELLANOS_____ Fecha: JULIO 2019

Aprobado por: _JUAN EDUARDO DIAZ_____ Fecha: _JULIO 2019

CONTROL DE REVISIONES/CAMBIOS			
No. Revisión	**Descripción de la Revisión/Cambio**	**Elaborado por**	**Fecha**
1	Primera Edición	Kriterion	Julio 2019
2	Actualización de contenido		