

1.0 OBJETIVO

Proporcionar el paso a paso de los procedimientos frente a novedades presentadas en los sistemas informáticos y lograr minimizar en lo más mínimo la inactividad y/o disponibilidad de los sistemas informáticos de Colviseg Del Caribe Ltda.

2.0 ALCANCE

Este Plan aplica a los sistemas informáticos de Colviseg Del Caribe Ltda, los cuales pueden ser: Servidores de Aplicaciones, Datos, Office365, Redes y todos aquellos equipos de cómputo ubicados en la sede principal de la Compañía.

3.0 DOCUMENTOS DE REFERENCIA

- Guía RUC.
- NTC-ISO 45001:2018
- NTC-ISO 9001:2015
- NTC-ISO 14001:2015
- Normas y Estándares BASC.
- PVP.
- Resolución DIAN 0000015 de Febrero del 2016.
- Decreto 1072 de 2015.

4.0 RESPONSABLES

Dirige:	Director de Informática y Tecnología.
Ejecuta:	Director Informática y Tecnología, Administrador del Sistema, Empleados en general.
Verifica:	Audidores internos / Auditores externos.

5.0 DEFINICIONES

PLAN DE CONTINGENCIA: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

PLAN DE CONTINUIDAD DE NEGOCIO (PCN): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

AMENAZA: Persona, situación o evento natural del entorno (Externo o Interno) que es visto como una fuente de peligro, catástrofe o interrupción.

VULNERABILIDAD: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la organización.

RIESGO: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la empresa.

RECURSO INFORMÁTICO: Elementos informáticos (Base de datos, Sistemas operacionales, Redes, Sistemas de información y Comunicaciones) que facilitan servicios informáticos.

INFORMACIÓN: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

USUARIOS TERCEROS: Todas aquellas personas naturales o jurídicas que no son funcionarios de Colviseg de Caribe Ltda., pero que por las actividades que realizan en la entidad, deban tener acceso a Recursos Informáticos.

ATAQUE CIBERNÉTICO: Intento de penetración de un Sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

BRECHA DE SEGURIDAD: Deficiencia de algún Recurso informático o Telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

6.0 DESARROLLO DEL PROCEDIMIENTO, INSTRUCTIVO O PROGRAMA

6.1 IDENTIFICACIÓN DE RIESGOS Y ANÁLISIS DE IMPACTO

6.1.1 Identificación de Riesgos y Amenazas

Hay eventos que al materializarse, pueden afectar algunos factores que integran la transversalidad de los diferentes procesos de Colviseg del Caribe LTDA, esos eventos están alineados a los riesgos identificados y constituyen una amenaza para la prestación del servicio:

- Desastres naturales
- Incendio
- Sabotaje
- Cortes de energía
- Ciberataques y/o delitos informáticos
- Fallas en el transporte
- Fallas en las comunicaciones
- Daño de hardware y Software.
- Caída de canales de internet
- Pérdida de información

6.1.2 Identificación de Recursos y Factores Críticos

En la Tabla 1 se describen los factores que pueden ser afectados por los riesgos y amenazas identificadas que impiden la continuidad de las operaciones, para la prestación del servicio.

FACTOR	DESCRIPCIÓN
Infraestructura	Infraestructura de hardware, servidores, equipos, elementos de redes lan, wan y todos los equipos que estén dentro de los sistemas informáticos de Colvisseg Del Caribe LTDA
Personal	Colaboradores directos o en misión que ejecutan actividades de los distintos procesos de la empresa.
Sistemas eléctricos	Sistemas e infraestructura que proporciona fluido eléctrico a todas las áreas de la organización.
Sistemas de información	Plataformas informáticas, softwares, office365, herramientas ofimáticas, utilizados para la realización de actividades de los procesos al interior de Colvisseg Del Caribe LTDA.
Medios de comunicación	Todos aquellos que nos suministran comunicaciones, canales de internet y datos.

Tabla 1. Factores críticos para la continuidad del negocio.

6.1.3 Análisis de Impacto

Como resultado del análisis de impacto se obtiene la información acerca de las funciones y procesos críticos del negocio que tengan que ver con los equipos o procesos tecnológicos, que puedan asegurar la continuidad de las operaciones informáticas de apoyo en la prestación de los servicios al de la organización.

6.2 ESTRATEGIAS DE CONTINUIDAD

Corresponden a las acciones que se tomarán con el objetivo de responder ante la materialización del riesgo para reestablecer las operaciones de Colviseg del Caribe LTDA, en el tiempo establecido una vez que ocurra alguna interrupción o falla en los procesos definidos como críticos y/o en uno o más de los factores identificados.

Las estrategias y pasos a seguir en caso de materialización de las amenazas identificadas y teniendo en cuenta los factores críticos establecidos, se encuentran en la **Tabla 2**.

POSIBLES SITUACIONES O RIESGOS QUE PODRÍAN AFECTAR EL DESARROLLO DE LA OPERACIÓN CONTRATADA	ESTRATEGIAS DE CONTINGENCIA Y/O CONTINUIDAD		
	ACTIVIDADES ANTES DEL EVENTO	ACTIVIDADES DURANTE EL EVENTO	ACTIVIDADES DESPUÉS DEL EVENTO
DESASTRE NATURAL (INUNDACIÓN, TERREMOTO)	Colviseg del Caribe LTDA, Garantizará la información de sus clientes e información de los usuarios y ERP, con el uso de la nube para la información de los usuarios. Para el caso de la información del software ERP y Kronos se utilizan medios digitales externos que permitan salvaguardar la información en servidores externos a las instalaciones.	En caso de materializarse este riesgo en las instalaciones de Colviseg del Caribe LTDA, se realizará el plan de evacuación y si es posible y necesario se cortará el suministro eléctrico y apagado de la planta para evitar daños eléctricos a los Servidores, Elementos de red y Equipos de cómputo.	<ul style="list-style-type: none"> • Se procede a verificar el grado de afectación de las instalaciones por parte del Administrador de sistemas y el director de IT, de los equipos y servidores validando su operatividad y daños producidos, dando prioridad a los utilizados para la prestación del servicio. Tiempo de 4 a 24 horas. • Inmediatamente se activará la central de monitoreo en la sede de Santa Marta (para reactivar el servicio de monitoreo), Tiempo de activación de 8 a 12 horas. • Se activará teletrabajo para dar continuidad a la prestación del servicio y dar respuesta de las solicitudes y novedades de los clientes, habilitando el acceso externo a office 365. Tiempo de activación de 4 a 8 horas.

PLAN DE CONTINGENCIA Y CONTINUIDAD INFORMÁTICA
INCENDIO

Las instalaciones donde están ubicadas los servidores y equipos críticos en Colviseg del Caribe LTDA, cuentan con Sistema contra incendio (Sistema de extintores) que se encuentra diseñado para ser acorde y suficiente a la capacidad instalada.

El área de informática garantizara la información de sus clientes e información de los usuarios y ERP, con el uso de la nube para la información de los usuarios. Para el caso de la información del software ERP y kronos, se utilizan medios digitales externos que permitan salvaguardar la información en servidores externos a las instalaciones.

El líder de la brigada procede a realizar el llamado a los organismos de socorro y a evacuar las instalaciones según la señal de alarma que se genera al interior de las instalaciones y está previamente socializada a todos los colaboradores de la empresa, el líder de la evacuación procede a realizar el recorrido por las instalaciones indicándole a los funcionarios las rutas para evacuar.

Al finalizar el proceso, se debe realizar el conteo VS la relación de los ingresos registrados en la minuta de ingreso y salida de personal.

- Para el caso de daño del servidor del software ERP, se procederá a activar equipo redundante realizando el montaje del backup almacenados remotamente o la copia local. De 24 a 48 horas si no se necesita repuesto.

- Se procede a verificar el grado de afectación de las instalaciones por parte del Administrador del sistema y el Director de IT, de los equipos y servidores validando su operatividad y daños producidos, dando prioridad a los utilizados para la prestación del servicio. Tiempo de 4 a 24 horas

- Inmediatamente se activará la Central de monitoreo en la sede de Santa Marta (para reactivar el servicio de monitoreo), Tiempo de activación de 8 a 12 horas.

- Se activará teletrabajo para dar continuidad a la prestación del servicio y dar respuesta de las solicitudes y novedades de los clientes, habilitando el acceso externo a office 365. Tiempo de activación de 4 a 8 horas.

- Para el caso de daño del servidor del software ERP se procederá a activar equipo redundante realizando el montaje del backup almacenado remotamente o la copia local. De 24 a 48 horas si no se necesita repuesto.

PLAN DE CONTINGENCIA Y CONTINUIDAD INFORMÁTICA

**SABOTAJE y/o
CIBER ATAQUES**

Las instalaciones de Colvisseg del Caribe LTDA, cuenta con un Sistema de seguridad para el uso y manejo de la información con los siguientes elementos:

Equipo UTM (Gestión Unificada de Amenazas). Este Firewall UTM es un cortafuego de red que engloba múltiples funcionalidades (servicios). Los servicios más relevantes son:

- Función de un firewall de inspección de paquetes.
- Función de VPN (para hacer túneles o redes privadas).
- Antispam (para evitar los correos no deseados o spam).
- Antiphishing (evitar el robo de información).
- Antispyware.
- Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías).
- Antivirus de perímetro (evitar la infección de virus informáticos en computadoras clientes y servidores)
- Detección/Prevención de Intrusos (IDS/IPS).

Se tiene una asignación de usuarios a cada empleado en la plataforma Office 365, lo que permite identificar la trazabilidad de su comportamiento dentro del sistema y realizar auditoria de los

Se activa el protocolo para la investigación establecido por Colvisseg del Caribe LTDA, para identificar las

vulnerabilidades materializadas que permitieron la materialización del sabotaje y/o ataque Cibernético a las instalaciones desde los diferentes frentes contemplados. (Usuarios, intrusos, software, hardware, entre otros).

Se procederá a aislar el equipo origen del virus y software de la red de la empresa.

Se bloquearán los accesos a las personas no deseadas y/o colaboradores que estén incumpliendo las políticas de seguridad de la información.

El equipo de Informática y Tecnología de Colvisseg del

Se procederá a investigar los daños ocurridos e impactos en el funcionamiento de los servicios para la ejecución de las actividades informáticas, si la cosa es inoperatividad se realizaran los siguientes:

- Daños de software, restauración de los equipos a un estado anterior para eliminar el virus no deseado. Si no funciona se procederá a la restauración de fábrica del Sistema operativo por completo e instalación de todos los software y aplicaciones. Tiempo de reactivación de 2 a 48 horas.
- Daños de Hardware:
 - Servidores: Activar equipo redundante y restablecer los servicios en ese tiempo de 2 a 48 horas, de igual forma se deberá realizar un informe de los daños producidos y la reparación o cambio total del equipo redundante, se socializaría a gerencia para su autorización.
 - Equipos de mesa: Realizar verificación de los daños y reemplazar las partes dañadas y/o cambio de equipo, (tiempo de 2 a 72 horas según la criticidad del caso) se socializaría a gerencia para su autorización.

PLAN DE CONTINGENCIA Y CONTINUIDAD INFORMÁTICA

archivos sospechosos y/o eliminación de información sensible.

Se tiene bloqueado el uso de los periféricos para la copia de la información, deshabilitando el uso de los puertos USB en cada uno de los equipos de cómputos utilizados por los colaboradores.

Todos los equipos cuentan con plataforma de antivirus con las siguientes funciones principales:

- Protegerse ante el ransomware.
- Bloquear los ataques dirigidos.
- Evitar la violación de datos.
- Detener los ataques sin archivos.
- Detectar las amenazas persistentes avanzadas.

Adicionalmente contamos con copias de seguridad de los servidores que se realizan 2 veces al día localmente y una externa todos los viernes, para los computadores de nuestros colaboradores, ellos disponen de 1 tb de almacenamiento en la nube para realizar sus copias de seguridad de la carpeta mis documentos.

Se realizan capacitaciones a los colaboradores en el uso, responsabilidades y medidas de prevención en la seguridad informática.

Caribe LTDA, procede a parchear la falla y a recuperar los datos, para posteriormente generar un informe de los datos que fueron sustraídos del sistema informático de la empresa, además notifica a los usuarios internos y externos el grado de afectación del Ciberataque materializado.

- Información: En caso de borrado de información se activarán las herramientas del panel de gobierno de información que nos permitirán administrar el ciclo de vida completo del contenido, desde la importación, el almacenamiento y la clasificación de los datos al inicio, su retención, supervisión y eliminación. Permitiéndonos restaurar información hasta 30 días después de eliminada, este gobierno funciona para la información de office 365 (Correo, OneDrive y SharePoint).

La Gerencia general de Colviseg del Caribe LTDA evalúa la situación con el informe de investigación y procede a realizar la respectiva denuncia ante los diferentes entes de control según el grado de impacto y afectación, igualmente la aprobación del presupuesto para la compra de elementos si se necesitan reemplazar.

PLAN DE CONTINGENCIA Y CONTINUIDAD INFORMÁTICA
CORTE DE ENERGÍA

Las instalaciones donde está ubicada Colviseg del Caribe LTDA, cuenta con planta eléctrica que permite reestablecer el fluido de energía, además que cada computador y servidor cuenta con una UPS para evitar la pérdida de la información en el evento en que falle el fluido eléctrico de manera intempestiva.

Un representante de la central de radio de Colviseg del Caribe LTDA, procede a llamar a la empresa que suministra el servicio de energía para saber las causas o motivos del corte de energía, y posterior a esto cada funcionario procede a guardar la información que está trabajando en el equipo de cómputo asignado para evitar que se pueda dar la pérdida de la información.

El área de Sistemas validará la operatividad de los equipos críticos que puedan tener afectación en la prestación del servicio.

Las instalaciones de Colviseg del Caribe LTDA, cuentan con un almacenamiento de combustible según la normatividad legal vigente y una capacidad de reserva de combustible para continuar la operación en 72 horas, si posterior a este tiempo no se ha reestablecido el fluido eléctrico, se procede a evaluar la viabilidad del traslado de la operación a una sede alterna fuera de la ciudad para garantizar la continuidad en la operación y la prestación del servicio de monitoreo de alarma. Tiempo de ejecución de 2 a 24 horas.

En caso de fallar el inicio de la planta eléctrica o presentarse un error de la UPS, se deberá llamar al Director de IT y/o al encargado del mantenimiento, los cuales se deben dirigir a la planta para validar la falla, si es fuera del horario laboral se deberá llamar y se deberán dar las indicaciones para reactivar los servicios, si no funciona se deberá proceder al sitio. En caso de fallas se deberán activar las siguientes actividades:

- Inmediatamente se activará la central de monitoreo en la sede de Santa Marta (para reactivar el Servicio de monitoreo). Tiempo de activación de 8 a 12 horas.
- Se activará teletrabajo para dar continuidad a la prestación del servicio y dar repuesta de las solicitudes y novedades de

PLAN DE CONTINGENCIA Y CONTINUIDAD INFORMÁTICA

			<p>los clientes, habilitando el acceso externo a office 365. Tiempo de activación de 4 a 8 horas.</p> <ul style="list-style-type: none"> Se trasladarán los servidores del Software ERP a la sede de Santa Marta u oficina alquilada en la sede de Barranquilla y se redireccionarán las conexiones al nuevo enlace. Tiempo de activación de 8 a 48 horas. <p>Se realizará seguimiento periódico al funcionamiento de los Servidores y Equipos críticos para garantizar su correcto funcionamiento.</p>
<p>FALLAS EN LAS COMUNICACIONES</p>	<p>Internet: En la sede principal y sucursales contamos con una red redundante que permitirá el funcionamiento si uno de los canales de internet presenta falla.</p> <p>Para la comunicación de los radios contamos con un stock de equipos de repuestos por si se presenta un daño físico.</p>	<p>El Director de IT y/o el Administrador del Sistema, inicia la evolución y el grado de impacto de las fallas y procede a notificar por medios escritos a los clientes, colaboradores y proveedores.</p> <p>Se activará el plan de continuidad que aplica para este.</p>	<p>Al riesgo de pérdida de internet el equipo UTM inmediatamente activará el canal secundario quedando en funcionamiento y sin trauma del servicio de internet, en caso de fallar el proceso automático el Director de IT y/o el Administrador del Sistema deberá validar las causas y reactivar el servicio. Posteriormente se deberá llamar al proveedor de internet para reportar la falla y realizar seguimiento de la reparación de esta.</p> <p>En caso de problema de comunicación radial, se deberá dirigir al sitio que presenta la falla y evaluar los daños presentados, en caso de ser en otra ciudad se contactará.</p>

			<p>La Junta Directiva de Colviseg del Caribe LTDA y la Gerencia General, evalúan la situación con el informe generado y se procede a realizar las respectivas denuncias ante los diferentes entes de control según sea el caso.</p> <p>Tan pronto se reestablezca la información, se les avisará de manera oportuna dándoles un parte de tranquilidad de que la prestación del servicio no se va a afectar.</p>
--	--	--	---

Tabla 2. Estrategias de Contingencia y/o Continuidad por Amenaza.

Adicional a las estrategias antes mencionadas, Colviseg del Caribe LTDA cuenta con Procedimientos para la Gestión del Área informática y Políticas que garantizan la Seguridad de la Información; así como con un Plan de Emergencia que contempla amenazas de origen técnico, social y natural, y describe los recursos y controles existentes para minimizar su materialización, así como las actividades a realizar en caso de que ocurran. Estos documentos se encuentran relacionados como complemento del presente Plan de Contingencia y Continuidad


7.0 DOCUMENTOS ASOCIADOS:

- Procedimiento de Informática, Código P-SE-02
- Políticas de Seguridad de la Información, Código D-SE-01
- Procedimiento de Prevención, preparación y respuesta ante emergencias, Código P-SI-11

8.0 CONTROL DE CAMBIOS

Fecha de actualización	Versión	Motivo de la actualización
22/10/2020	01	Creación del Documento con base en las normas mencionadas.

9.0 CONTROL DE DOCUMENTO

	ELABORÓ	REVISÓ	APROBÓ
NOMBRES Y APELLIDOS	Juan Carlos Delgado	Andrea Barraza A.	Daiyana Serrano
CARGO	Director de Informática y Tecnología	Analista SGI	Gerente General
FECHA	22-10-20	22-10-20	22-10-20
FIRMA		Andrea S. Barraza A.	