|  |
| --- |
| Plan de Continuidad de Negocio - CLI |
|  | PUESTO | NOMBRE | FECHA |
| ELABORADO POR: | Asistente de Calidad | Rubí Ramos | 16/04/2021 |
| REVISADO POR: | Jefe de Seguridad y Calidad | Ricardo Alarcón | 16/04/2021 |
| APROBADO POR: | Gerente General | Giovanni Klein | 16/04/2021 |

1. **Objetivo**

Establece la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.

1. **Alcance**

Todos los Procesos de CLI.

1. **Responsabilidad**

Responsable del presente documento es la Gerencia General

1. **Abreviaturas**

N.A.

1. **Referencias**

N.A.

1. **Definiciones**

Plan de Continuidad de Negocio (PCN) establece la continuidad de una organización desde múltiples perspectivas: sistemas informáticos, recursos humanos, mobiliario, comunicación, logísticas, infraestructuras físicas y otros. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.

1. **Condiciones generales**
	1. Determinar las amenazas a las que está expuesta la organización**:** Robo de información sensible, inundación o aniegos, perdida de suministro eléctrico, caída del servidor de correo y otras amenazas que implican una indisponibilidad de los procesos del alcance.
		1. PRO-SG-056 – Atención de Casos Críticos o Especiales
		2. PRO-SIG-015 – Contingencia y Emergencia
		3. PRO-TI-028 – Copia de respaldo informático (Backup)
		4. PRO-TI-047 – Contingencia Informática
		5. Robos, asaltos o perdidas de los bienes
		6. Falla del suministro eléctrico
		7. Caída o Falla de Base de Datos
		8. Caída o Falla del servidor de correo
		9. Caída o Falla del servicio de Internet
		10. Caída o Falla del Sistema – CLINET (Servidor / Ataques cibernéticos)
		11. Falla o presencia de errores en el software externo (SINTAD)
		12. Perdida de la información – BACK UP
		13. Aniegos
		14. Incendios
		15. Desastres naturales
		16. Pandemia Mundial por causas del COVID-19 y otros futuros virus
2. **Descripción del proceso**

Para el presente Plan de Continuidad de Negocio, debemos considerar que nos ayudará en:

* Mantener el nivel de servicios en los límites definidos
* Establecer un periodo de recuperación mínimo
* Recuperar la situación inicial antes de cualquier incidente de seguridad
* Analizar los resultados y los motivos de los incidentes
* Evitar que las actividades de la empresa se interrumpan
	1. **PRO-SG-056 – Atención de Casos Críticos o Especiales**
		1. Objetivos: Definir la metodología a seguir para la adecuada atención de los casos críticos o especiales, tales como las novedades, quejas de los clientes, reclamos o sucesos especiales ocurridos en la organización.
		2. Alcance: Es aplicable a todas las situaciones (ocurridas o por ocurrir) que puedan afectar drásticamente a las personas, instalaciones, operaciones o servicios de la organización.
		3. Condiciones Generales:
1. Se consideran casos críticos o especiales las novedades, las quejas de los clientes, los reclamos y/o los sucesos especiales ocurridos en la organización.
2. Dentro de las novedades se encuentran las operaciones o actividades nuevas que desarrollará la empresa, así como también la planeación del desempeño de la organización ante cambios bruscos de nuestras operaciones, debido a modificaciones normativas importantes de los organismos que rigen nuestra actividad.
3. Para los casos de quejas y/o reclamos de los clientes, el ESC debe informar de este hecho, enviando esta información al correo cli.incidencias@cliandina.com.
4. Así mismo deberá el ESC registrar la respuesta enviada al cliente, en el correo cli.incidencias@cliandina.com.
5. Los sucesos especiales comprenden la atención que brindaremos a casos específicos que pueden estar relacionados a temas comerciales, operativos y/o que afecten a la seguridad y salud laboral dentro de la organización.
6. En este último punto se consideran también los servicios no conformes, los cuales deben tratarse según lo señalado en el presente procedimiento.
	* 1. Plazo: Entre 10 minutos y 24 horas
	1. **PRO-SIG-015 – Contingencia y Emergencia**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia y emergencia.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en las medidas de protección del Sistema de Gestión en Control y Seguridad o del Sistema Integrado de Seguridad.
		3. Condiciones Generales: En el caso de tener que alertar al personal se utilizará la función de la central telefónica de altavoz general.

En los casos que se requiera dar declaraciones de lo acontecido (ante autoridades, prensa, etc.), solo se realizará bajo la autorización de la Gerencia.

1. ***Desperfectos e Emergencias imprevistas***
2. ***Desvío de Rutas de la Unidad Vehicular***
3. ***Procedimientos ante Robos o intentos de asaltos***
4. ***Bloqueos de vías, Disturbios, Perturbaciones civiles y retrasos de la Unidad Vehicular***
5. ***Accidente de Tránsito*** (Colisión o Choque)
6. ***Falla Mecánica***
7. **Fallas del equipo de refrigeración**
8. ***Siniestros Unidades Vehiculares***
9. ***Vulneración de precintos de Seguridad***
10. ***Apertura de Mercadería***
11. **En caso de robo y/o asalto al Auxiliar de Despacho**
12. **Primeros Auxilios ante Accidentes de Trabajo**
	* 1. Plazo: Se dará según el tipo de contingencia registrada.
	1. **PRO-TI-028 – Copia de respaldo informático (Backup)**
		1. Objetivos: Describir las actividades a realizar para la obtención correcta de las copias de respaldo (Backup) de la información que se procesa diariamente en los servidores de CLI.
		2. Alcance: Aplica al proceso de copia de respaldo de la información de los equipos de la empresa.
		3. Condiciones Generales:
13. El Backup a la información se realiza diariamente.
14. Los Backups contienen los siguientes grupos de archivos: Bases de datos de los distintos servidores, correos electrónicos y Archivos de Usuarios.
	* 1. Plazo: Entre 10 minutos y 1 hora dependiendo del tamaño de la base de datos.
	1. **PRO-TI-047 – Contingencia Informática**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia informática.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: Las contingencias informáticas consideradas en el presente documento son las siguientes:
15. Falta o corte de energía en las instalaciones de la empresa.
16. Falta o falla en el servicio de internet y/o correo electrónico.
17. Falla o presencia de errores en el software externo utilizado por la empresa.
18. Pérdida de la información.
	* 1. Plazo: Las contingencias informáticas consideradas en el presente documento son las siguientes:
19. Grupo electrógeno se activa inmediatamente.
20. Desde 10 minutos hasta más de 1 hora dependiendo del tamaño la base de datos
21. Dependiendo de la falla entre 10 minutos y 1 hora
22. Recuperación de información depende del tamaño de base de datos entre 10 minutos y 1 hora.
	1. **Robos, asaltos o perdidas de los bienes**
		1. Objetivos: Establecer las pautas a seguir en caso de un aniego en las instalaciones de CLI.
		2. Alcance: Es aplicable a todo CLI
		3. Condiciones Generales: Contamos con un sistema de seguridad, el cual cuenta con un sistema biométrico para ingreso a las instalaciones y una garita de vigilancia.
		4. Plazo: Se activan la Póliza 3D de inmediato.
	2. **Falla del suministro eléctrico:**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia informática.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: PRO-TI-047 – Contingencia Informática
		4. Plazo: Se activan automáticamente los UPS que dan energía a los servidores en un período de 20 a 30 minutos y a su vez se enciende en automático el grupo electrógeno.
	3. **Caída o Falla de Base de Datos**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del proceso.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales:
		4. Plazo: Contamos con un servidor de réplica para estos casos, el cual se ejecuta en un rango aproximado de 20 a 30 minutos.
	4. **Caída o Falla del servidor de correo**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del proceso.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: Llenado de buzón de correos electrónicos y Envío de correos electrónicos superando la capacidad máxima por usuario y/o grupal
		4. Plazo: Para la descongestión se debe esperar un rango de tiempo que en el mejor de los casos se da en media hora o caso contrario superando la hora.
	5. **Caída o Falla del Servicio de Internet:**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia informática.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: PRO-TI-047 – Contingencia Informática
		4. Plazo: Se activa automáticamente la línea de internet de backup (American móvil) contratada con otro proveedor, siendo imperceptible al usuario.
	6. **Caída o Falla del Sistema – CLINET (Servidor / Ataques cibernéticos)**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del proceso.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales:
23. Servidor: Generación de errores por falta de verificación en los nuevos procesos que suben.
24. Ataques cibernéticos: Uso de un puerto común (Ejm. Puerto 80).
	* 1. Plazo:
25. Servidor: Se reinicia el servidor por un aproximados de 05 minutos.
26. Ataques cibernéticos: Se rastrea el IP atacante y se procede a bloquearlo, adicional a ello contamos con un firewall (delante de nuestros servidores) que detecta ataques a nuestros servicios con el fin de evitar de que estos se vean afectados.
	1. **Falla o presencia de errores en el software externo (SINTAD)**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia informática.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: PRO-TI-047 – Contingencia Informática
		4. Plazo: Se comunica el área de Sistemas con nuestro proveedor de software externo y se les permite realizar vía conexión remota las correcciones necesarias para restablecer el servicio.
	2. **Perdida de la información – BACK UP**
		1. Objetivos: Establecer las pautas a seguir para la puesta en marcha del procedimiento de contingencia informática.
		2. Alcance: Es aplicable ante los casos de amenazas comprobadas o fallos en los sistemas informáticos de la empresa.
		3. Condiciones Generales: PRO-TI-047 – Contingencia Informática
		4. Plazo: Se cuenta con copias de respaldo backup de la información almacenada en los servidores, en los discos lógicos y en la carpeta BKP\_SISTEMAS instalada para la información personal de cada usuario.
	3. **En caso de Aniegos:**
		1. Objetivos: Establecer las pautas a seguir en caso de un aniego en las instalaciones de CLI.
		2. Alcance: Es aplicable a todo CLI
		3. Condiciones Generales: CLI cuenta con un sistema de alarma de aniegos, los cuales se encuentran ubicados en los SSHH del 1er piso y 3er piso.
		4. Plazo: Se activan automáticamente la alarma de aniegos y dependiendo de la gravedad se activa la Póliza de Multiriesgo.
	4. **En caso de Incendios:**
		1. Objetivos: Establecer las pautas a seguir en caso de un aniego en las instalaciones de CLI.
		2. Alcance: Es aplicable a todo CLI.
		3. Condiciones Generales: CLI cuenta con un sistema de alarma de aniegos, los cuales se encuentran ubicados en los 03 pisos de las instalaciones.
		4. Plazo: Se activan automáticamente las alarmas de incendio, se procede a retirar al personal que se encuentre en las instalaciones de CLI y se activa la Póliza de Multiriesgo.
	5. **Desastres Naturales:**
		1. Objetivos: Establecer las pautas a seguir en caso de un aniego en las instalaciones de CLI.
		2. Alcance: Es aplicable a todo CLI.
		3. Condiciones Generales: NA
		4. Plazo: Se activan la Póliza 3D de inmediato.
	6. **Pandemia Mundial por causas del COVID-19 y otros futuros virus**
		1. Objetivos: Establecer las pautas a seguir en caso de un aniego en las instalaciones de CLI.
		2. Alcance: Es aplicable a todo CLI.
		3. Condiciones Generales: Pandemia Mundial
		4. Plazo: Se realizan planes de prevención frente al virus y una reorganización por parte de la Gerencia General.
27. **Control de cambios**

N.A.

1. **Anexos**

N.A.