Municipalidad Distrital de Carmen de la Legua-Reynoso
**"Año del Fortalecimiento de la Soberanía Nacional"**
GERENCIA MUNICIPAL

# RESOLUCIÓN DE GERENCIA MUNICIPAL N° 301-2022-GM/MDCLR

Carmen de la Legua Reynoso, 16 de diciembre de 2022

**VISTOS:**

El Informe N° 220-2022-MDCLR/GAF-SGTI de fecha 21.11.2022 de la Sub Gerencia de Tecnología de la Información, Informe N° 0194-2022-GAF/MDCLR de fecha 23.11.2022 de la Gerencia de Administración y Finanzas, Memorándum N° 02615-2022-GAF/MDCLR de fecha 14.11.2022 de la Gerencia de Administración y Finanzas, Memorándum N° 587-2022-GPP/MDCLR de fecha 29.11.2022 de la Gerencia de Planeamiento y Presupuesto, Memorándum N° 2685-2022-GAF/MDCLR de fecha 02.12.2022 de la Gerencia de Administración y Finanzas, Informe N° 350-GAJ/MDCLR de fecha 05.12.2022 de la Gerencia de Asesoría Jurídica, e Informe N° 208-2022-GAF/MDCLR de fecha 07.12.2022 de la Gerencia de Administración y Finanzas;

**CONSIDERANDO:**

Que, conforme a los artículos 194° y 195° de la Constitución Política del Perú, modificado por las Leyes de Reforma Constitucional Ley N° 27680 y 30305 concordante con el articulo I y II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley N° 27972, Las Municipalidades son órganos de gobierno promotores del desarrollo local, con persona jurídica de derecho públicos y plena capacidad para el cumplimiento de sus fines; con autonomía política, económica y administrativa en asuntos de su competencia, autonomía que radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico, concordante con el Artículo II del Título Preliminar de la Ley N° 27972 – Ley Orgánica de Municipalidades;

Que, de acuerdo al Artículo 6° de la Ley N° 27972 – Ley Orgánica de Municipalidades, la alcaldía es el órgano ejecutivo del gobierno local y el alcalde es el representante legal de la Municipalidad y su máxima autoridad administrativa, y según el artículo 20° del mismo cuerpo legal, establece que son atribuciones del alcalde numeral 20 "Delegar sus atribuciones políticas en un regidor hábil y las administrativas en el Gerente Municipal"; texto concordable con el artículo 27° y 39° de la citada norma, cuando señala que la administración bajo la dirección y responsabilidad del Gerente Municipal; las gerencias resuelven los aspectos administrativas a su cargo a través de resoluciones y directivas, respectivamente;

Que, el artículo 27° de la Ley N° 27972 – Ley Orgánica de Municipalidades, determina que la Administración Municipal está bajo la dirección y responsabilidad del Gerente Municipal, funcionario de confianza a tiempo completo, correspondiente a la alcaldía de las funciones ejecutivas;

Que, la Ley Marco de Modernización de la Gestión del Estado, Ley N° 27658, en su artículo 4° declara que el proceso de modernización de la Gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de recursos públicos;

Que, de conformidad con el numeral 4.1 del artículo 4° (Proceso de Modernización de la Gestión Pública) del Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, aprobado por Decreto Supremo N° 123-2018-PCM, la modernización de la gestión pública consiste en la selección y utilización de todos aquellos medios orientados a la creación de valor público en una determinada actividad o servicio a cargo de las entidades públicas. Se crea valor público cuando las intervenciones públicas, que adoptan la forma de bienes, servicios o regulaciones, satisfacen las necesidades y expectativas de las personas, generando beneficios a la sociedad; y se optimiza la gestión interna a través de un uso más eficiente y productivo de los recursos públicos, para directa o indirectamente, satisfacer las necesidades y expectativas de las personas, generando beneficios a la sociedad;

Que, de conformidad con el Decreto Legislativo N° 1412, se aprueba la Ley de Gobierno Digital, con el objeto de establecer el marco de gobernanza del gobierno digital en el estado y el régimen jurídico por el uso de tecnologías digitales en la Administración Pública;

Que, el artículo 30° del Decreto Legislativo N° 1412 establece que la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;

Que, la Ley N° 28551, Ley que establece la obligación de elaborar y presentar Planes de Contingencia, dispone que todas las personas naturales y jurídicas de derecho privado o público y conducen y/o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar la su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle;

Que, mediante Informe N° 220-2022-MDCLR/GAF-SGTI de fecha 21.11.2022 la Sub Gerencia de Tecnología de la Información estando a lo establecido en la normatividad vigente elabora el "Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Carmen de la Legua Reynoso", para lo cual la Gerencia de Administración y Finanzas a través de Memorándum N° 02615-2022-GAF/MDCLR de fecha 24.11.2022 corre traslado a la Gerencia de Planeamiento y Presupuesto para su evaluación y conformidad;

Que, con Memorándum N° 587-2022-GPP/MDCLR de fecha 29.11.2022 la Gerencia de Planeamiento y Presupuesto estima conveniente su aprobación;

Que, mediante Memorándum N° 2685-2022-GAF/MDCLR de fecha 02.12.2022 la Gerencia de Administración y Finanzas derivó todos los actuados a la Gerencia de Asesoría Jurídica solicitando la respectiva opinión legal, el mismo que es atendido mediante Informe N° 350-2022-GAJ/MDCLR de fecha 05.12.2022, en la cual opina que resulta VIABLE, que mediante Resolución de Gerencia Municipal se apruebe la "Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Carmen de la Legua Reynoso", conforme al proyecto adjunto de la Gerencia de Administración y Finanzas mediante Informe N° 0194-2022-GAF/MDCLR de fecha 21.11.2022;

Que, con Informe N° 208-2022-GAF/MDCLR, de fecha 07.12.2022, la Gerencia de Administración y Finanzas remite los actuados a la Gerencia Municipal con la finalidad aprobar mediante Resolución Gerencial la "Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Carmen de la Legua Reynoso";

Que, estando a lo expuesto, y en uso de las facultades conferidas en el Artículo Primero de la Resolución de Alcaldía N° 349-2019-MDCLR; y Resolución del Alcaldía N° 188-2021/MDCLR que resuelve ampliar la delegación de facultades y atribuciones en materia administrativa al Gerente Municipal;

**SE RESUELVE:**

**ARTÍCULO PRIMERO. – APROBAR,** el "PLAN DE CONTINGENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CARMEN DE LA LEGUA REYNOSO".

**ARTÍCULO SEGUNDO. – ENCARGAR,** a la Gerencia de Administración y Finanzas y Sub Gerencia de Tecnología de la Información, el seguimiento y cumplimiento de las medidas establecidas en el presente Plan.

**ARTÍCULO TERCERO. – DISPONER,** a la Sub Gerencia de Tecnología de la Información la publicación de la presente Resolución en el portal de transparencia de la Municipalidad Distrital de Carmen de la Legua Reynoso.

**REGÍSTRESE, COMUNÍQUESE, PUBLIQUESE Y CÚMPLASE**

MUNICIPALIDAD DISTRITAL DE CARMEN DE LA LEGUA REYNOSO
LIC. ADM. CESAR IGOR CAMACHO CABALLERO
GERENTE MUNICIPAL

# PLAN DE CONTINGENCIA DE TECNOLOGIA DE LA INFORMACION

## MUNICIPALIDAD DISTRITAL DE CARMEN DE LA LEGUA REYNOSO

| | Nombre | Cargo | Firma | fecha |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

# INDICE

# I. INTRODUCCION

El objetivo estratégico del área de la SUBGERENCIA DE TECNOLOGIA DE LA INFORMACIÓN es brindar sistemas y servicios confiables a sus clientes internos y externos. Un sistema confiable es aquel con el que se puede contar para brindar servicios a sus usuarios toda vez que estos servicios se requieran.

Sin embargo, construir y operar sistemas confiables es un proceso continuo que incluye complejas interdependencias entre los siguientes componentes de una empresa o institución.

- Infraestructura física.
- Equipos con Software base.
- Comunicaciones.
- Software aplicativo.
- Datos y procedimientos operacionales.
- Personal operativo y especializado.

¿Para qué se desarrolla un Plan de Contingencia?

El Plan de Contingencia se desarrolla para prever la recuperación optima posible en la eventualidad que ocurra una pérdida de capacidad operativa, una pérdida de datos o se produzca una falla en las medidas de seguridad.

Uno de los beneficios de contar con un plan de contingencia es que al existir un planeamiento de recuperación del evento o desastre, se evita la pérdida de tiempo valioso que se debe emplear en la recuperación de la misma.

Nota: los planes de contingencia no se deben concentrar en eventos límites como regla general, mientras más adversa sea el impacto de un evento (destrucción total de un edificio, por terremoto, fuego o inundación) menor es la probabilidad de su ocurrencia.

La complejidad y profundidad del plan está directamente relacionada a la complejidad del sistema, su costo y su importancia en el cumplimiento de la misión de la organización. Por lo tanto se debe evitar el "sobre - planeamiento", haciendo que el plan de contingencia consista en una descripción de una serie de "acciones" orientadas a la recuperación del sistema.

En el grafico N° 1 se muestran los componentes que constituyen la arquitectura de un sistema confiable que toda municipalidad debe tener.

| | |
|---|---|
| Personal técnico especializado | Usuarios |
| Personal de soporte administrativo | |
| Procesos institucionales | Áreas operativas y de soporte |
| Procesos de soporte | |
| Información y datos institucionales | Datos institucionales |
| | Áreas operativas |
| Sistemas aplicativos | Software aplicativo |
| | Desarrollo de sistemas |
| Red de área local (LAN) | Comunicaciones |
| Red de área ampliada (WAN) | Soporte técnico |
| Comunicación con agencias | |
| Correo electrónico e internet | |
| Estaciones e impresoras | Equipos y Software base |
| Software base y motor de base de datos | Soporte Técnico |
| Edificio y oficinas | Infraestructura física |
| Alimentación eléctrica | Administración lógica |
| Aire acondicionado | |
| Mobiliario y facilidades | |

**Grafico N° 1 – Arquitectura de sistemas confiables**

**Dentro de las causas de las caídas de los sistemas podemos mencionar.**

- **Daños en discos duros:** los daños varían en seguridad, desde pequeñas fallas que son reparadas con herramientas de software, a graves daños físicos que destruyen el disco duro en forma permanente. Particiones de discos dañadas o corruptas contribuyen a la perdida de datos. Hay que tener en cuenta que cualquier dispositivo mecánico eventualmente falla.
- **Fallas del equipo:** Los discos son solamente una parte funcional de una computadora, si otro componente falla tal como una tarjeta madre, memoria, tarjeta de red, etc. El sistema puede estar inoperativa por horas o días aunque la información almacenada en los discos no está en peligro.
- **Fallas en el software:** Software corrupto (generalmente copias piratas que se utilizan ilegalmente) o incompatible puede producir una caída en los servidores.
- **Errores de usuario o administrador:** los errores humanos también pueden causar la caída del sistema. Un usuario o administrador puede causar borrado de archivos de sistemas, directorios, o modificación de datos.
- **Virus:** los sistemas se pueden poner fuera de servicio causado por un virus. Los virus son un real y potente amenaza para la infraestructura de datos.

# CAPITULO I

## OBJETIVOS DEL PLAN DE CONTINGENCIA

- **La SUBGERENCIA DE TECNOLOGIA DE LA INFORMACIÓN** busca con el plan de contingencia, mantener un plan escrito y explicito de las políticas y normas generales para mantener la continuidad de la operación del servicio de sistemas y comunicaciones, en la eventualidad de una falla mayor de equipos, del Software, de las comunicaciones, pérdida de los datos relevantes, destrucción temporal o permanente de las instalaciones o ausencias prolongadas de personal clave.

Como se muestra en el "grafico N° 2 – Esquema de seguridad y Contingencia" con el Plan de Contingencia y Recuperación de Desastres se busca reducir las fuentes de contingencia minimizando así el riesgo de ocurrencia de un evento limite o extremo.

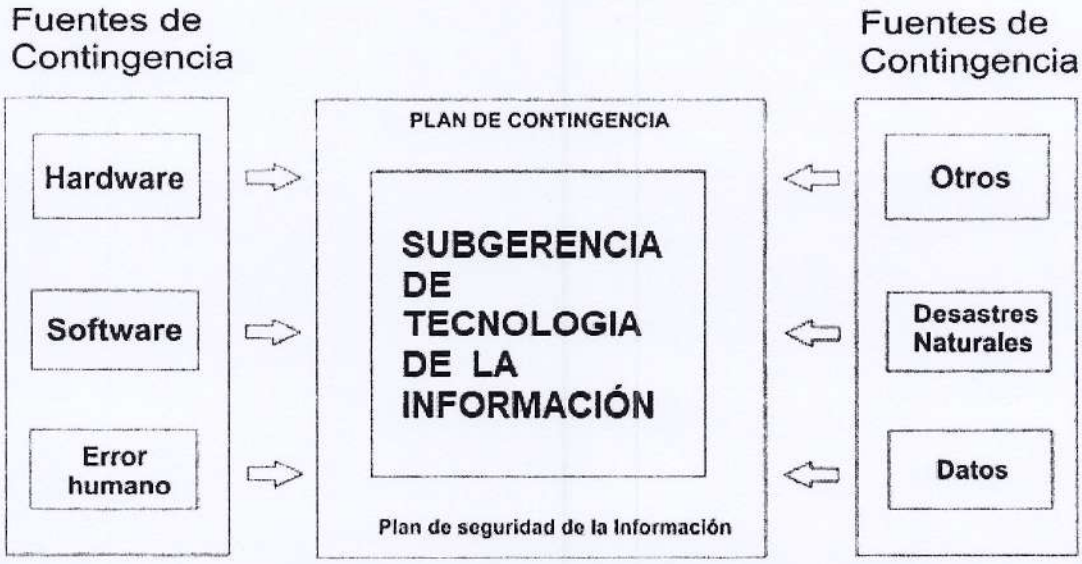



**Gráfico N°2- Esquema de seguridad y contingencia**

## ASPECTOS GENERALES

A continuación se presentan los aspectos generales considerados, tales como la definición de los procesos a ser soportados por el plan, la identificación de los usuarios afectados, la metodología empleada, la

estructura organizacional para ejecutar el plan y las responsabilidades de la Sub Gerencia.

1. **Definición de los procesos a ser soportados por el plan.**
   Para la implementación del plan de contingencia y recuperación de desastres, se recomienda tener en cuenta la criticidad de los procesos internos, de tal manera que se ponga mayor énfasis en aquellos más críticos. A continuación se muestra un cuadro con los procesos y subprocesos y su respectivo nivel de criticidad.

| Subproceso | Proceso Principal | Criticidad |
|---|---|---|
| | | Nivel |
| Administración Tributaria (Rentas, Coactivos y Fiscalización) y plataforma. | Proceso de Recuperación y Data | Alta |
| Tecnología de la Información | Administración de recursos institucionales. | Alta |
| Planeamiento y Programación Multianual de Inversiones | Gestión de proyectos | Alta |
| Desarrollo Urbano y Económico | Proceso de Recuperación y Data | Alta |
| Contabilidad | Soporte de Gestión | Media |
| Tesorería | Soporte de Gestión | Media |
| Logística | Soporte de Gestión | Baja |
| Planeamiento y Presupuesto | Soporte de Gestión | Baja |
| Administración | Soporte de Gestión | Baja |
| Control Patrimonial | Soporte de Gestión | Baja |
| Imagen Institucional | Proceso de Recuperación y Data | Baja |

2. **Metodología empleada.**
   La metodología más utilizada para el desarrollo del presente Plan de contingencia, es la Metodología de Seguridad y Continuidad del Servicio (MSC), que se muestra en la figura N°03.

El presente Plan de Contingencia se realiza con las siguientes pautas metodológicas.

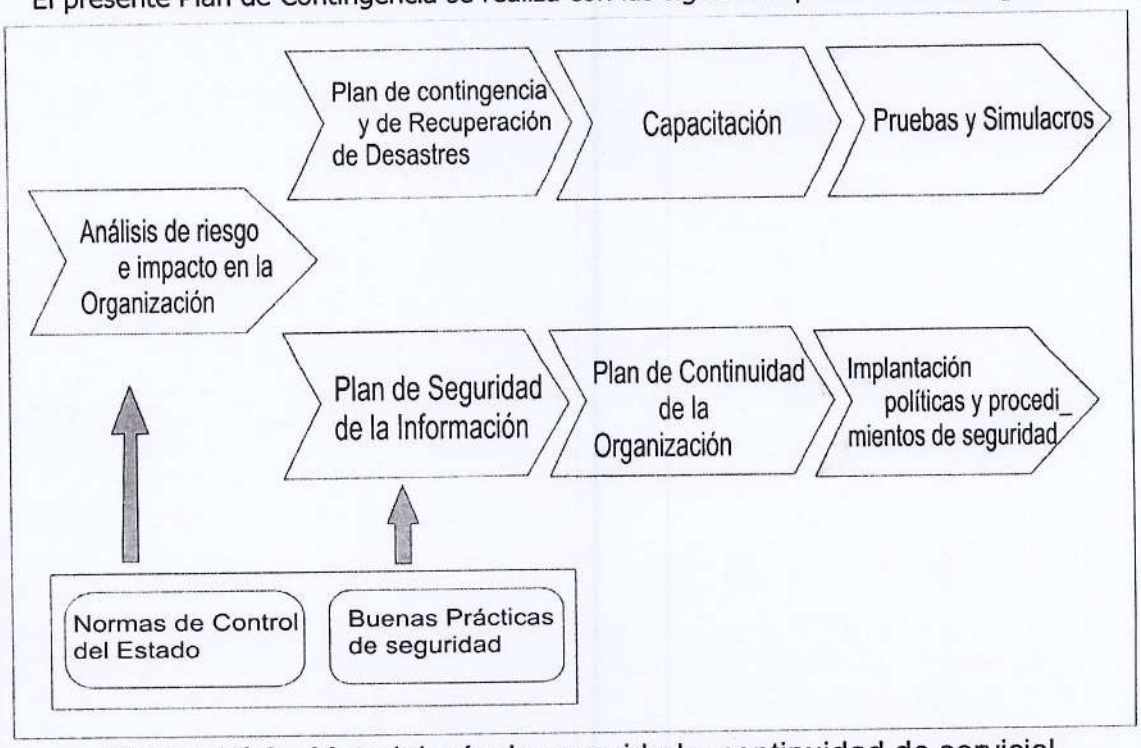
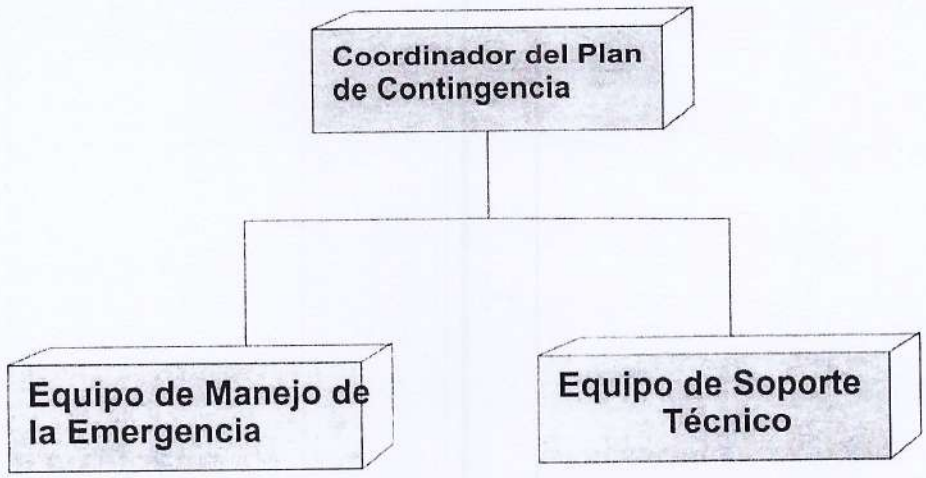



Gráfico N° 3 - Metodología de seguridad y continuidad de serviciol

- ✓ Políticas de seguridad
- ✓ Riesgo
- ✓ Centro de computo
- ✓ Plan de continuidad Operacional
- ✓ Plan de contingencia y de recuperación de desastres.

## 3. Identificación de la estructura Organizacional requerida para ejecutar el plan de contingencia.



### 3.1 Coordinador del plan de contingencia.

La SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN asumirá dentro de sus funciones, la coordinación del plan de Contingencia. Sus responsabilidades principales serán:

- Actuar como el contacto primario en caso de contingencias.
- Contactar a todo el personal de soporte involucrado en el esfuerzo de reposición.
- Proveer a todo el personal de soporte una copia actualizada del plan de contingencia.
- Contactar a las siguientes personas, tan pronto como sea posible: Gerente de Administración, Encargado de Soporte Técnico, Encargado de Desarrollo y procesos.
- Ejecutar el plan de contingencia.
- Mantener actualizada la bitácora de contingencias.

### 3.2 Equipo de manejo de emergencias.

Este equipo estará integrado por: El especialista de redes y comunicaciones, el especialista de procesos y el especialista de administración de sistemas y/o las personas que la Municipalidad decida asignar. Sus responsabilidades principales serán:

- Evaluación de la contingencia o del daño.
- Proveer rápidamente de un informe detallado del estado de la contingencia al Coordinador del Plan de Contingencia.
- Coordinar los esfuerzos de recuperación o reposición de la contingencia.
- Contactar a los recursos externos y/o proveedores necesarios para restaurar los servicios afectados por la contingencia.
- Proveer de información relativa a la contingencia al personal afectado.
- Asegurar que todo el personal de soporte que se requiera ha sido contactado para proveer asistencia.
- Determinar el tiempo que tomara restaurar las operaciones completamente.

### 3.3 Equipo de Soporte técnico

Este equipo estará integrado por las unidades de Soporte Técnico y comunicaciones. Sus responsabilidades serán:

- Determinar los equipos, Software u otros periféricos si han sido dañados.
- Revisar la evaluación de prioridades del plan y revisar que actividades son críticas y cuáles no, así como determinar quién es responsable de cada una de ellas y contactarlos.
- Ejecutar los procedimientos necesarios para trasladar los quipos a un nuevo ambiente y de ser el caso adquirir otros nuevos.
- Ejecutar los procedimientos necesarios para restaurar el Software y las aplicaciones, el Hardware y los equipos de comunicaciones.
- Notificar a los usuarios del servicio de la contingencia y dar un estimado de tiempo necesario para la reposición de las operaciones.
- Coordinar con el proveedor indicado el servicio de la reposición inmediata de los equipos con características técnicas similares o superiores a los siniestrados, dentro de los plazos y tiempo de respuesta previstos según contrato.
- Realizar todas las llamadas telefónicas requeridas.

## 4. Los respaldos de la Información

La recuperación de archivo de datos y el reemplazo de un equipo principal requiere la autorización de la Sub Gerencia De Tecnología de La Información.
La información de la municipalidad constituye uno de sus recursos de mayor importancia, por ello se considera que se deberá tener controles para asegurar la confiabilidad de dicha información.

### 4.1 Requerimientos de respaldo de información.

Uno de los aspectos de mayor relevancia con respecto a la seguridad de los sistemas de información (backup) que permitan su restauración inmediata ante cualquier eventualidad y aseguren la continuidad de las operaciones.
Las pérdidas de datos pueden ser generadas por altas o bajas en la fuente eléctrica, desastres naturales, simples accidentes, sabotaje, falla de los sistemas de información o fallas del equipamiento.
La SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN de la Municipalidad deberá tener en cuenta que el respaldo (backup) hecho sin ningún reporte de error no significa que fue resguardado correctamente. Las restauraciones parciales deben realizarse al menos una vez al mes.

### 4.2 Estrategias de respaldo de la información en la Municipalidad de Carmen de la Legua Reynoso.

Las acciones concernientes al generar los backup en la Municipalidad de Carmen de la Legua son las siguientes:

- Se realizara copias de seguridad en Discos Duros, conteniendo los archivos de los sistemas con la Base de Datos. Se Utilizaran DVD cuando el Backup no supere los 4Gb.
- Se utilizara respaldados por los servidores en la nube pueden restaurarse rápidamente, permitiendo a la institución obtener acceso inmediato a los archivos o sistemas deseados.
- El protocolo de creación de backups será según el cuadro que se describe en el procedimiento de acceso y Generación de backups.
- Se mantendrá una copia de respaldo del Sistema Operativo y de Base de Datos en el Disco Local principal de operación. Esto para garantizar un mejor tiempo de restauración en caso de una contingencia mayor.

### 4.3 Periodicidad de respaldo

La Sub Gerencia De Tecnología De La Información deberá ejecutar procedimientos de backups de la información de la Municipalidad de Carmen de la Legua según las siguientes recomendaciones.

- **Respaldo diario por producto**

  El proceso de backups deberá ser luego del proceso de cierre diario y se recomienda se realice automáticamente a las 11:00p.m el proceso de backups, deberá generar dos copias idénticas. Estas copias se trasladan independientemente al Data Center de la SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN y la otra para su custodia fuera de la entidad.

  Los sistemas que se indican a continuación deberán ser respaldados diariamente ya que son objeto de constante actualización por parte de usuarios.

- **Respaldo semanal por producto**

  Con esta frecuencia se debe efectuar copias de seguridad de la siguiente información en Discos Duros:

  **1.** La información creada por los usuarios y almacenados en sus respectivas computadoras personales, sean documentos de texto, hojas de cálculo, gráficos o cualquier otro tipo de archivo serán

respaldados según el Procedimiento de acceso y Generación de Backups.

**2.** Los correos electrónicos (archivo *.pst) de cada usuario serán respaldados siguiendo el Procedimiento de Acceso y Generación de Backups.

**3.** Los Fuentes y Ejecutables de todos los sistemas en PHP, Visual Basic 6.0, visualFox y BD Oracle y Sql server 2014 que se copiaran diariamente siguiendo el procedimiento de Acceso y Generación de Backups.

- **Respaldo mensual del producto**

**1.** La copia de información del sistema contable, comprende la información al cierre de mes y los asientos contables correspondientes, la información de sistemas del SIAF, del sistema de recuperaciones y los que defina en su oportunidad por necesidad de seguridad de la información o criterio de la SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN.

**2.** Se realizara una copia de toda la información.

### 4.4 Almacenamiento de los respaldos de los medios Magnéticos.

Los Discos Duros contenidas las copias de respaldo de la información relevante de la Municipalidad se deberán almacenar en dos lugares distintos para incrementar la seguridad de la perdida de información. El primero debe ser un espacio especialmente acondicionado para este fin en las instalaciones del centro de cómputo de la institución y técnicamente denominado Discoteca (lugar de seguridad física en la sala de servidores o Data Center). Un segundo deberá ser las Discotecas de una institución externa que brinde los servicios de almacenamiento, custodia de los Discos Duros backup o el respaldo basado en la nube. Por tratarse de activos de gran valor para la Institución almacenados en medios magnéticos, estos lugares deberán cumplir con las especificaciones técnicas de seguridad. Estas especificaciones están basadas en controles de características como:

- Controles de temperaturas.
- Detectores de humedad.
- Puerta con cerradura de combinación o dispositivo biométrico.

## 5. Plan de ejecución.

El plan de ejecución tiene por finalidad establecer los procedimientos que permitan responder a las contingencias que afecten el normal funcionamiento de los servicios de sistemas y comunicaciones de la Municipalidad de Carmen de la Legua Reynoso.

Los elementos que conforman el plan de ejecución son los relativos a:

- Escenarios de Contingencia y Prioridades de Reposición.
- Procedimientos de Contingencia según las Fuentes de Origen.

## 5.1 Escenarios de Contingencias y Prioridades de Reposición.

### 5.1.1 Escenario de Contingencias.

El plan de contingencia deberá considerar la provisión para el servicio de sistemas y comunicaciones de la Municipalidad de la Plataforma Informática necesaria que le permita continuar sus operaciones ante un evento extraordinario o imprevisible que inutilice completamente el funcionamiento de los servidores de producción ubicados en las oficinas.

Se consideran los siguientes escenarios de Contingencias severas o desastres:

- ✓ Desastre del centro de cómputo de la SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN.
- ✓ Desastre de oficinas administrativas.

| N° | Escenario | Respuesta | Observación |
|---|---|---|---|
| 1. | • Inhabilitación severa del centro de cómputo de la Municipalidad de Carmen de la Legua Reynoso. | • Reposición por parte del proveedor de un nuevo servidor de producción dentro de los tiempos de respuesta estipulados según contrato. | La operatividad en las oficinas de la Municipalidad de Carmen de la Legua Reynoso se verá afectadas por un plazo no mayor de 2 días. |

En caso de que ocurra un desastre en el Centro de cómputo de la Municipalidad de Carmen de la Legua Reynoso, que impida el normal funcionamiento del Servidor de Producción se ha considerado la inclusión de cláusulas, ya sea en el contrato de alquiler o compras que indiquen

claramente que ante la pérdida total o parcial del servidor, se garantice la reposición ó restablecimiento de un equipo con similares o superiores características técnicas que el servidor siniestrado en un tiempo no mayor a 24 horas puesta la alarma.

### 5.1.2 Prioridades de Reposición

Los recursos disponibles serán usados para recuperar y reponer funciones basadas en su criticidad e importancia para la continuidad de la operación de la organización. A continuación identificamos los sistemas a ser repuestos en orden de prioridad.

| N° | SISTEMA | CRITICIDAD |
|---|---|---|
| 1 | Sistema de RENTAS | Alta |
| 2 | Sistema de SIAF | Alta |
| 3 | Sistema de SIGA | Alta |
| 4 | PC's de usuarios | Alta |
| 5 | Sistema de Trámite Documentario | Alta |
| 6 | Sistema de Recursos Humanos | Media |
| 7 | Sistema de CORREOS | Media |
| 8 | Sistema de Backup | Media |
| 9 | Otros sistemas | Baja |

| Ítem | Prioridad | Tiempo Máximo de Parada | Tiempo Máximo de Rehabilitación |
|---|---|---|---|
| 1 | Alta | 1 día | 2 día |
| 2 | Media | 1½ día | 2 día |
| 3 | Baja | 1 día | 3 días |

Dónde:

- **Tiempo de parada:** Es el tiempo máximo que se puede tolerar antes de implementar el plan de contingencia.
- **Tiempo de rehabilitación:** Es el máximo que puede transcurrir desde el inicio del plan hasta el reinicio de las operaciones.

## 5.2 Tareas para verificar el correcto funcionamiento de la estrategia de respaldo.

Es responsabilidad del equipo de Soporte Técnico el asegurar el funcionamiento de los equipos computacionales y comunicaciones, así como de los procesos críticos.

Por lo tanto este equipo deberá:

- ✓ Ejecutar los procedimientos necesarios para trasladar los equipos a un nuevo ambiente y de ser necesario adquirir otros nuevos.
- ✓ Restaurar el Software base y las aplicaciones una vez que estén debidamente instalados los equipos computacionales y de comunicaciones y de haberse verificado la operación de la red alterna.

- ✓ Restaurar los datos de las aplicaciones a partir de los medios magnéticos que forman parte del backup externo.

- ✓ Asegurar el funcionamiento de los módulos de los sistemas a ser restaurados, mediante la participación de los usuarios principales de los procesos críticos a restaurar.

## 5.3 Procedimientos de Respuestas a Contingencias

En este punto se desarrollan los procedimientos de contingencia desde la fase de notificación de la contingencia hasta los procedimientos de rehabilitación según la fuente de origen y estable de la contingencia.

### 5.3.1 Procedimiento general de respuesta a contingencias

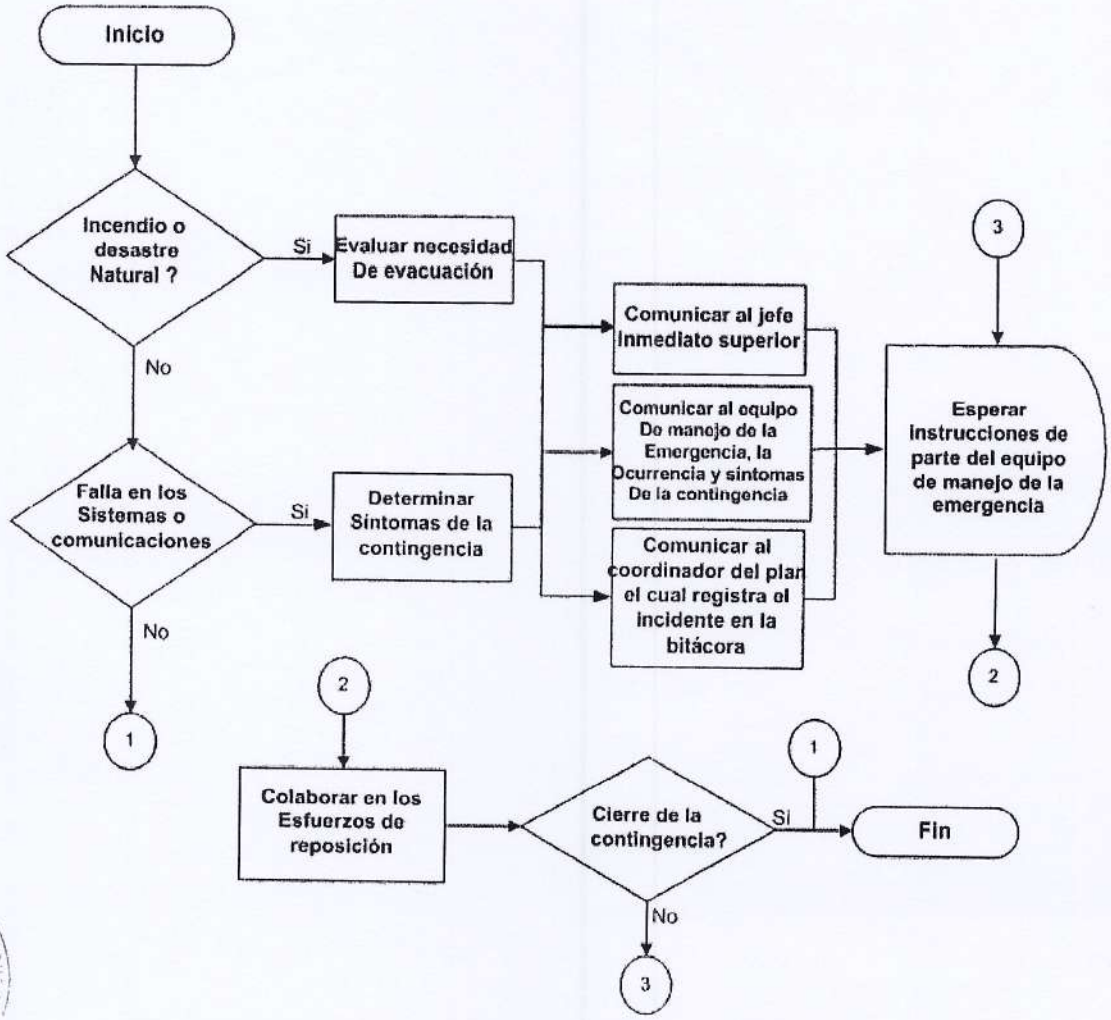
En el siguiente gráfico se muestran los procedimientos de Notificación, Activación y rehabilitación. Los cuales serán descritos a detalle en el presente plan.

| Procedimiento de NOTIFICACION de contingencia | Procedimiento de ACTIVACIÓN de contingencia | Procedimiento de REHABILITACION de contingencia |
|---|---|---|
| | | |
| Objetivo: Notificar la ocurrencia de una contingencia al equipo de emergencia y al coordinador del plan de contingencia. | Objetivo: Evaluar la contingencia y activar los procedimientos de rehabilitación de contingencia. | Objetivo: La reparación efectiva y confiable de la contingencia según su fuente de origen en el menor tiempo posible. |
| Usuario: Todos los equipos de trabajadores de administración. | Usuario: Equipo de manejo de emergencia. | Usuario: Equipo de soporte técnico. |

### 5.3.1.1 Procedimiento de Notificación de una contingencia.

El procedimiento de notificación de una contingencia permite poner en marcha el plan de contingencia, dando a conocer la ocurrencia de una contingencia al equipo de manejo de emergencias o a quien se designe.

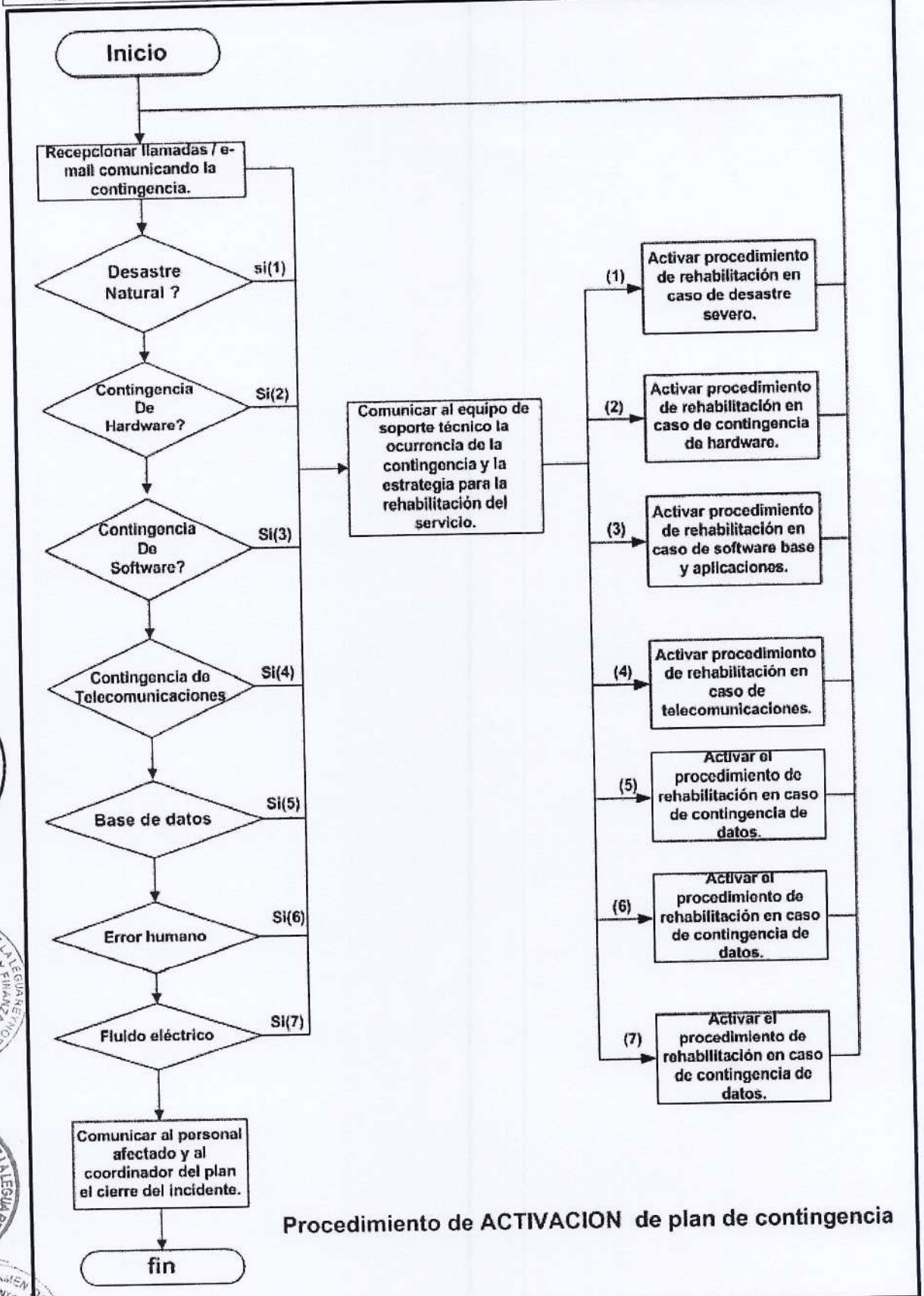
En la siguiente imagen se muestra el procedimiento de **notificación** de contingencias.




**Procedimiento de NOTIFICACION de contingencias**

### 5.3.1.2 Procedimiento de Activación del Plan Contingencia.

El Procedimiento de Activación del Plan de Contingencias, se encarga de la evaluación de las fuentes y causas de la Contingencia por parte del equipo de manejo de emergencias o persona que se asigne, así como el grado de criticidad de la misma.




Procedimiento de ACTIVACION de plan de contingencia

### 5.3.1.3 Procedimiento de Rehabilitación de Contingencia

Las fuentes de contingencias cubiertas por este plan y las acciones a ejecutar para cada una de ellas se detallan a continuación. Estas fuentes de contingencias se refieren usualmente a diferentes grados dentro de 7 categorías: Hardware, Software, Error Humano, pérdida de datos, desastre severo, Telecomunicaciones y Fluido Eléctrico. La causa de la perdida se determina luego del diagnostico que se realiza, siendo el primer objetivo del plan de ejecución determinar el grado de perdida, el impacto en la misión y las técnicas para minimizar este riesgo.

Es importante también definir los niveles de contingencia según su impacto directo en la Institución. Los niveles de contingencia los define el Equipo de Manejo de Emergencias o persona que se asigne y en caso de contingencia severa, el traslado al Centro de Procesamiento de Respaldo deberá ser autorizado por la SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN.

| Calificación | Nivel de severidad | Situación |
|---|---|---|
| Verde | No causa impacto en el servicio | Operación normal.<br>Los equipos, software base y aplicaciones operan sin problemas |
| Amarillo | Impacto mínimo en el servicio | Falla aislada en equipos, Software base y aplicaciones.<br>El problema o defecto causa una pérdida mínima en el servicio. |
| Rojo | Impacto serio en el servicio | Falla parcial o total de equipos, Software base y aplicaciones que impiden la producción.<br>El problema o defecto causa una pérdida severa en el servicio. |
| Negro | Impacto critico en el servicio | Contingencia extrema (terremoto, incendio, vandalismo, etc.) que afectan la infraestructura, equipos o al personal. El problema causa una perdida completa del servicio o impide la producción. |

**Calificaciones según el impacto**

A continuación se presentan los procedimientos de rehabilitación del plan de contingencia.

| Procedimientos |
|---|
| Procedimiento de rehabilitación en caso de desastre severo |
| Procedimiento de rehabilitación en caso de contingencia de equipos críticos – Hardware. |
| Procedimiento de rehabilitación en caso de contingencia de Software base y aplicaciones. |
| Procedimiento de rehabilitación en caso de contingencia de comunicaciones. |
| Procedimiento de rehabilitación en caso de contingencia de datos. |
| Procedimiento de rehabilitación en caso de error humano. |
| Procedimiento de rehabilitación en caso de falla de fluido eléctrico. |

# Procedimientos

## CAPITULO II

### PROCEDIMIENTO DE ACCESO Y GENERACIÓN DE BACKUPS

**1. OBJETIVO**

Establecer el acceso a los usuarios al sistema (datos y programas), determinar qué información deberá ser resguardada de acuerdo a la criticidad para la operación del sistema y fijar locaciones de respaldo internos o externos para la conservación de los back-ups.

**2. ALCANCE**

El presente procedimiento es administrado por el SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN y es ejecutado por el personal de Soporte Técnico.

**3. DEFINICIONES**

3.1 **Información**.- Activo especial de la organización soportada a través del sistema.

3.2 **Back-up**.- Copia de seguridad de ficheros (archivos) o datos de forma que estén disponibles en caso que un fallo produzca la pérdida de los originales.

3.3 **Criticidad**.- La incidencia que tiene un Hardware o su información contenida dentro de la operación de la empresa.

3.4 **Programas**.- Software ejecutable que reciben datos y generan información.

3.5 **Data Center**.- Lugar del centro de información donde se ubican los servidores, equipos de seguridad, equipos de comunicación de acceso a personal restringido.

3.6 **File Server**.- Llamado también servidor de archivos, lugar donde los usuarios guardaran sus archivos (documentos de texto, hojas de cálculo, gráficos, diseños, etc) importantes para que sean resguardados por el área de SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN. Es responsabilidad del usuario copiar dicha información a este ambiente.

## 4. CONDICIONES BASICAS

Se debe tener presente:

4.1 Proteger el entorno de PC's o redes locales con protección de acceso (paswords), protección antivirus, servidor de archivos y backups de seguridad.

4.2 Para los backups de seguridad lo ideal será contar con equipos de Tapes Backups y Discos Duros pero también la información puede ser copiada en DVD, CD, discos duros externos o respaldo basado en la nube.

4.3 Solicitar formatos de envió o precintos de seguridad para los backup respectivos si la información es enviada a través de seguridad externa o se debe tener una bóveda segura externa al Data Center con las condiciones de ambiente climáticas necesarias.

## 5. DESCRIPCION DEL PROCEDIMIENTO

Es responsabilidad del SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN o persona que designe, gestionar:

## 5.1 Acceso a la información

5.1.1 Recibir los requerimientos de las Gerencias y Subgerencias para el acceso de los usuarios a la red y a programas de acuerdo a las necesidades de utilización.

5.1.2 Coordinar con las Gerencias y Subgerencias los accesos a los programas a ser instalados o configurados en los usuarios y las restricciones cuando sean aplicables.

5.1.3 Asignar a los usuarios autorizados por las Gerencias o Subgerencias el acceso a datos y/o programas mediante su nombre de usuario y contraseña.

5.1.4 Verificar el acceso a los programas mediante la realización de por lo menos tres inspecciones por año y contrastarlo con la información de inventario de programas y cuando sea necesario lo actualizara.

5.1.5 Proteger las PC's de programas externos (virus) que puedan afectar su funcionamiento mediante el uso de programas antivirus debidamente autorizados los cuales serán utilizados por los usuarios.

## 5.2 Generación de backups

5.2.1 Coordinar con la empresa que brinda el servicio de custodia de los backups el día y la hora del traslado y solicitar el formato de envió y los precintos de seguridad para los backups respectivos. De no existir el servicio de custodia de backups, los backups serán enviados a la bóveda externa al Municipio o el respaldo basado en la nube.

5.2.2 Rotulas los discos colocando el numero de la semana / fecha a la que corresponde la información que se guardara de acuerdo al calendario del backup, y realizar los backups de la información del sistema fuera de la hora del trabajo de oficina (no realizar backups en caliente).

5.2.3 Registrar en el calendario de backup la semana / fecha correspondiente a los backups, proceder a llenar el formato de envió al proveedor que brinda la custodia y programar la fecha del próximo envió.

5.2.4 El dia establecido a la hora programada, recibir a la empresa de custodia, la caja y los formatos necesarios para el retiro de los backups llenados y firmados según sea el requerimiento, en caso de no contar con el servicio de custodia externo se enviara los backups de reemplazo a la bóveda de seguridad externa a la Sede Municipal.

5.2.5 Proceder abrir la caja y retirar los discos. Luego colocar las nuevas copias de seguridad y entregar el formato debidamente llenado

5.2.6 Archivar los documentos necesarios para el sustento de la operación.

**5.3 Es responsabilidad del SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN o persona que designe.**

5.3.1 Realizar periódicamente el backup de seguridad de la información de los servicios de la municipalidad.

5.3.2 Controlar la ejecución del programa semestral del mantenimiento preventivo.

5.3.3 La información de copia de seguridad son:

a. Base de datos de los drivers de los sistemas, periodicidad diaria (en lo posible).
b. Fuentes y programas principales, se deberá sacar backups una vez al mes.
c. La copia de seguridad del servidor de archivos será cada dos semanas.
d. La copia de seguridad de la información de los correos electrónicos en servidor serán cada semana.

# CAPITULO III

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE DESASTRE SEVERO

### 1. OBJETIVO

Recuperar la capacidad operativa de la Municipalidad, en el caso de que el local sufra alguna contingencia que imposibilite el funcionamiento del servicio en dichas instalaciones.

### 2. ALCANCE

Es responsabilidad del Equipo de Manejo de Emergencias controlar el cumplimiento del presente procedimiento.

El equipo de Soporte Técnico es responsable de efectuar la rehabilitación del servicio para reiniciar las operaciones de la Municipalidad en el más breve plazo.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia

- ✓ Plan de recuperación de desastres.

## 4. CONDICIONES BÁSICAS

Se debe tener:

4.1 Contar con materiales, herramientas y repuestos.

4.2 Ambiente e infraestructura adecuada.

4.3 Contar con implementos de seguridad.

## 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 El equipo de Manejo de la Emergencia con la ayuda del Equipo de Soporte Técnico realizaran las siguientes labores:

- Diagnostico y detección de la inhabilitación del local.
- Determinación del grado de pérdida y el impacto del sistema.
- Se informara al coordinador del plan sobre el estado del incidente y a los usuarios el tiempo esperado de normalización de operaciones.

5.3 El responsable de Soporte Técnico Informara al SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN de la Municipalidad el estado de la contingencia.

5.4 El equipo de manejo de emergencias coordinara con el equipo de Soporte Técnico el inicio de las acciones para instalar y configurar de forma inmediata el servidor de producción ya sea el proporcionado por la empresa que se contrato para tal fin u otro diferente.

5.5 Luego se procederá a restaurar el Software base, Base de Datos y los datos con la información contenida en los discos backup ubicadas en el servidor de producción (la restauración se debe trabajar con los últimos backups realizados).

5.6 Una vez operativo el Servidor de Producción y los equipos, se restablecerá el proceso y el servicio.

5.7 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO IV

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE CONTINGENCIA DE EQUIPOS CRÍTICOS

### 1. OBJETIVO

Asegurar la reparación efectiva y confiable de los equipos críticos (servidores y estaciones) para devolverlo a su estado normal en el menor tiempo posible.

### 2. ALCANCE

En caso de ocurrir una contingencia que lleve a la pérdida de un equipo (servidor o estación) se ha establecido el siguiente procedimiento.

El equipo de Soporte Técnico es responsable de efectuar la reparación y puesta en operatividad de los equipos.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.
- ✓ Plan de mantenimiento preventivo de Hardware.
- ✓ Lista maestra de Hardware.
- ✓ Procedimiento para el mantenimiento de Hardware.

### 4. CONDICIONES BÁSICAS

Se debe contar:

4.1 Contar con materiales, herramientas y repuestos.

4.2 Ambiente e infraestructura adecuada.

4.3 Contar con implementos de seguridad.

### 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 El equipo de Soporte Técnico realizará las siguientes labores:

- Diagnostico y detección de la falla del equipo.

- Determinación del grado de pérdida y el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informara al equipo de manejo de la emergencia el estado del incidente y el tiempo estimado de la normalización de las operaciones.

5.3 Reparación de Estación de Trabajo

- Si se opta por la reparación del equipo, Soporte Técnico solicitara el repuesto de la parte dañada, para proceder a realizar el reemplazo.
- Se procederá con el cambio de la parte dañada.
- Se realizaran los diagnósticos y pruebas de funcionamiento.

5.4 En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.3

5.5 Sustitución de Equipo de Trabajo.

- Se procederá a sustituir el equipo por contingencia.
- Se configurara el equipo de contingencia.
- Se realizaran los diagnósticos y pruebas de funcionamiento.

5.6 Una vez que el equipo de Soporte Técnico a puesto operativo el/los equipos se procederá a efectuar el cierre del incidente comunicando al equipo de manejo de emergencias y al coordinador del plan de contingencia.

5.7 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO V

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE CONTINGENCIA DE SOFTWARE BASE Y APLICACIONES

### 1. OBJETIVO

Asegurar el restablecimiento del Software y aplicaciones relevantes en el menor tiempo posible, ante un evento en el cual un Software base y/o las aplicaciones se dañen o corrompan.

## 2. ALCANCE

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento. El Equipo de Soporte Técnico se encargara de ejecutar los procedimientos necesarios para restaurar, reinstalar o reconfigurar el Software dañado o perdido.

## 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.
- ✓ Lista maestra de Hardware.

## 4. CONDICIONES BÁSICAS

Se debe contar:

3.1 Contar con materiales, herramientas y repuestos.

3.2 Ambiente e infraestructura adecuada.

3.3 Contar con Software instaladores y licencias respectivas.

## 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 El equipo de Soporte Técnico realizará las siguientes labores:

- Diagnostico y detección de la falla del equipo.
- Determinación del grado de pérdida y el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informara al equipo de manejo de la emergencia el estado del incidente y el tiempo estimado de la normalización de las operaciones.

5.3 Se procederá a la instalación del Software con problemas y de ser necesario se restaurara la información perdida.

5.4 Se realizaran los diagnósticos y pruebas de funcionamiento

5.5 En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.2

5.6 De pasar bien se informará al SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN a fin de proceder a entregar el equipo y ponerlo operativo y se comunicará a los usuarios afectados el restablecimiento del servicio.

5.7 Reparación de la estación de trabajo.

- Se procederá a la instalación del Software en contingencia.
- Se realizaran los diagnósticos y pruebas de funcionamiento.
- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.2

5.8 Una vez que el equipo de Soporte Técnico a puesto operativo el/los equipos se procederá a efectuar el cierre del incidente comunicando al equipo de manejo de emergencias y al coordinador del plan de contingencia.

5.9 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO VI

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE CONTINGENCIA DE COMUNICACIONES

### 1. OBJETIVO

Asegurar el restablecimiento de las comunicaciones de datos a su estado de operación normal en el menor tiempo posible.

### 2. ALCANCE

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento. El equipo de Soporte Técnico es responsable de efectuar la reparación y puesta en operatividad de los equipos.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.
- ✓ Lista maestra de Hardware.

## 4. CONDICIONES BÁSICAS

Se debe contar:

4.1 Contar con materiales, herramientas y repuestos.
4.2 Ambiente e infraestructura adecuada.
4.3 Contar con implementos de seguridad.

## 5. SELECCIÓN DEL HARDWARE

Se empleara un sistema de criticidad. Este sistema clasifica al Hardware de acuerdo a la incidencia que tiene dentro de los procesos de la institución o según el tipo de información que administre. Para determinar el nivel de criticidad del Hardware se recurre al siguiente cuadro.

| Código | Incidencia |
|---|---|
| 1 | Un Hardware **no debe fallar**. Si esta máquina falla paraliza el proceso del flujo de información incluyendo la perdida de datos. |
| 2 | Un Hardware que **no debería fallar**, continúa siendo un Hardware importante pero una avería en este equipo no tendrá un fuerte impacto en la ejecución del proceso. |
| 3 | Todos los demás equipos cuyas fallas afectarían en forma mínima en el proceso y/la información. |

5.1 Para todo Hardware con **criticidad 1 y 2** se ha elaborado un programa semestral de mantenimiento preventivo.

5.2 Todo Hardware con **criticidad 3**, no se determina una acción preventiva por no ser considerado relevante para la continuidad del proceso siempre se efectuara una acción correctiva.

## 6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

6.2 El equipo de Soporte Técnico realizará las siguientes labores:

- Diagnostico y detección de las comunicaciones.
- Determinación del grado de pérdida y el impacto de la misma.

6.3 Falla en equipos de comunicaciones (Router, Switchs, firewall).

- El equipo de Soporte Técnico realizará el reemplazo de equipos defectuosos, en caso de ser alquilados con la clausula respectiva de remplazo en caso de pérdida.
- Se realizaran los diagnósticos y pruebas de funcionamiento.
- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 6.2

6.4 En caso de fallas externas el equipo de Soporte Técnico se comunicara con el/los proveedores del servicio de comunicaciones para determinar el tiempo estimado de reposición.

6.5 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO VII

## PROCEDIMIENTO DE REHABILITACION EN CASO CONTINGENCIA DE DATOS

### 1. OBJETIVO

Recuperar la información de los sistemas en el menor tiempo posible, ante un evento por el cual estos se dañen o corrompan.

### 2. ALCANCE/ RESPONSABILIDADES

La recuperación de archivos de datos, puede ser ejecutada con la autoridad del Administrador de red. Es responsabilidad del Coordinador del Plan de Contingencia de controlar el cumplimiento del presente procedimiento. El equipo de Soporte Técnico se encargara de ejecutar los procedimientos necesarios para restaurar, los datos perdidos o corruptos.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.
- ✓ Procedimiento de acceso y generación de backups.

### 4. CONDICIONES BÁSICAS

Se debe Contar:

4.1 Contar con materiales, herramientas y repuestos.

4.2 Ambiente e infraestructura adecuada.

4.3 Contar con implementos de seguridad.

## 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 El equipo de Soporte Técnico realizará las siguientes labores:

- Diagnóstico y detección de la falla del equipo.
- Determinación del grado de pérdida y el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informará al equipo de manejo de la emergencia el estado del incidente y el tiempo estimado de la normalización de las operaciones.

5.3 Reparación de Estación de Trabajo

- Se solicitará la última copia de respaldo y restaurará la información del usuario.
- Se realizarán los diagnósticos y pruebas de funcionamiento.
- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.2

5.4 Falla del Servidor Aislado

- Se solicitará la última copia de respaldo y restaurará la información del servidor en contingencia.
- De ser necesario se procederá a la reparación del equipo usando el procedimiento de rehabilitación de la Municipalidad del presente plan.
- Se realizarán los diagnósticos y pruebas de funcionamiento.
- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.4

5.5 Falla de múltiples servidores.

- Revisar la lista de prioridades de reposición.
- Se repiten los pasos del punto 5.4 las veces que sean necesarios.
- Se realizarán los diagnósticos y pruebas de funcionamiento.

5.6 Una vez que el equipo de Soporte Técnico a puesto operativo el/los equipos se procederán a efectuar el cierre del incidente comunicando al equipo de manejo de emergencias y al coordinador del plan de contingencia.

5.7 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO VIII

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE ERROR HUMANO

### 1. OBJETIVO

Asegurar la reposición del servicio de sistemas en el menor tiempo posible en el caso de fallas por error humano.

### 2. ALCANCE/ RESPONSABILIDADES

Es responsabilidad del SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN (Coordinador del Plan de Contingencia) controlar el cumplimiento del presente procedimiento y es ejecutado por el equipo de Soporte Técnico / Administradores de Base de Datos u sistemas. El procedimiento es aplicado a todo dispositivo electrónico, de interconexión y electromecánico que utilicen algún tipo de Software y/o base de datos.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.

### 4. CONDICIONES BÁSICAS

Se debe contar:

4.1 Contar con materiales, herramientas y repuestos.

4.2 Ambiente e infraestructura adecuada.

4.3 Contar con implementos de seguridad.

### 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 Error Humano no Intencional.

- El equipo de Soporte Técnico junto con el usuario involucrado determina el grado de perdida en el servicio.
- Se siguen los procedimientos de Rehabilitación de Hardware, Software o datos relevantes según sea el caso.
- Se realizarán las pruebas de funcionamiento.

- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.2.

5.3 Error Humano Intencional

- El jefe inmediato superior del usuario involucrado aplicara las sanciones administrativas pertinentes.

- Se repiten los pasos 5.2.

5.4 Una vez operativo el/los equipos se procederá a efectuarse el cierre del incidente comunicando al Equipo de la Emergencia y coordinador del plan de contingencia.

5.7 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.

# CAPITULO VIX

## PROCEDIMIENTO DE REHABILITACIÓN EN CASO DE FLUIDO ELÉCTRICO

### 1. OBJETIVO

Recuperar el servicio de fluido eléctrico en el menor tiempo posible, ante un evento por el cual este sea interrumpido.

### 2. ALCANCE/ RESPONSABILIDADES

Es responsabilidad del SUB GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN (Coordinador del Plan de Contingencia) controlar el cumplimiento del presente procedimiento, el equipo de Soporte Técnico se encargara de ejecutar los procedimientos necesarios para restaurar el servicio de fluido eléctrico.

### 3. DOCUMENTOS A CONSULTAR

- ✓ Plan de contingencia.
- ✓ Programa semestral de mantenimiento preventivo de Hardware.
- ✓ Lista maestra de Hardware.
- ✓ Plan de mantenimiento de Hardware.

### 4. CONDICIONES BÁSICAS

Se debe contar:

4.1 Contar con materiales, herramientas y repuestos.

4.2 Ambiente e infraestructura adecuada.

4.3 Contar con implementos de seguridad.

4.4 Contar con equipo de UPS y baterías externas en buen estado y mantenimiento respectivo.

4.5 contar con equipos de grupo electrógeno y combustible necesario.

## 5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Recepcionar la llamada del Equipo de Manejo de Emergencias, indicando las posibles fuentes de contingencia.

5.2 Fluido eléctrico a cargo de los equipos interrumpibles de energía UPS. Verificar el estado actual de las baterías y el tiempo de autonomía.

5.3 Verificación de las baterías externas para el UPS.

5.4 El Equipo de Soporte Técnico realizara el encendido manual del grupo electrógeno. De no existir grupo electrógeno continuar con ítem 5.5 y obviar el ítem 5.8.

5.5 El Equipo de Soporte Técnico realizara la detección y diagnostico de la falla.

5.6 Falla Externa.

- El equipo de Soporte Técnico se comunicara con el proveedor del servicio de fluido eléctrico para determinar el tiempo de reposición del servicio.
- El equipo de Soporte Técnico informara el tiempo estimado de reposición al equipo de manejo de emergencias.

5.7 Falla Interna

- El Equipo de Soporte Técnico se encargara de la revisión del tablero de transferencia eléctrica.
- En caso de no detectar la falla se solicitara el apoyo de electricistas externos a la institución.
- Se realizaran las pruebas de funcionamiento.
- En caso de seguir presentando algún problema se vuelven a repetir los pasos desde el ítem 5.5

5.8 Una vez superada la contingencia, el equipo de Soporte Técnico se encargara del apagado del grupo electrógeno.

5.9 El coordinador de contingencia registrara el incidente en una bitácora de contingencia.