

RESOLUCIÓN DE GERENCIA GENERAL

N° 124 -2023-GG-EPS.EMAPICA S.A.

Ica, 05 de mayo de 2023.

VISTO:

El Informe N° 077-2023-EPS EMAPICA S.A./GG/GAF de fecha 26 de abril de 2023 y el Informe N° 0126-2023-EPS EMAPICA S.A./GAF/OTIC de fecha 25 de abril de 2023; y,

CONSIDERANDO:

Que, la EPS EMAPICA S.A., es una empresa prestadora de servicios de saneamiento de accionariado municipal, constituida como empresa pública de derecho privado, bajo la forma societaria de sociedad anónima, cuyo accionariado está suscrito y pagado en su totalidad por las Municipalidades Provinciales de Ica y Palpa, posee patrimonio propio y goza de autonomía administrativa, económica y de gestión. Su ámbito de competencia es la localidad de Ica, Parcona, Los Aquijes y Palpa. Incorporada al Régimen de Apoyo Transitorio (RAT) por Consejo Directivo del OTASS a través de su Sesión N° 019-2016 de fecha 06 de septiembre de 2016, acuerdo que fue ratificado por el Ministerio de Vivienda, Construcción y Saneamiento – MVCS mediante la Resolución Ministerial N° 345-2016-VIVIENDA de fecha 06 de octubre del 2016;

Que, en el marco del Reglamento de Organización y Funciones (ROF) de la EPS EMAPICA S.A., en el artículo 13° numeral 13.7, la Gerencia General en ejercicio de sus funciones está facultada para "Proponer o aprobar las directivas, guías, manuales, protocolos, instructivos y procedimientos de administración, recursos humanos, finanzas, presupuesto, inversión pública, relaciones institucionales y otras, en concordancia con lo que establezca el directorio, así como la normativa de dichas materias que le son aplicables, dando cuenta al Directorio de la aplicación de las mismas";

Que, mediante Informe N° 0126-2023-EPS EMAPICA S.A./GAF/OTIC, de fecha 25 de abril de 2023, el jefe de la Oficina de tecnología de la Información y Comunicaciones, remite el "Plan de Contingencia Informático", como un documento de carácter confidencial que describe los procedimientos que debe seguir su oficina en caso de emergencias, a fin de asegurar el funcionamiento de los sistemas Informáticos de la empresa, para su aprobación mediante acto resolutivo;

Que, mediante Informe N° 077-2023-EPS EMAPICA S.A./GG/GAF de fecha 26 de abril de 2023, el gerente de la Gerencia de Administración y Finanzas, luego del análisis y revisión del referido plan, solicita su aprobación, considerando que el objetivo de la misma es establecer la organización, normas y procedimientos a seguirse para garantizar la operatividad de la empresa; así como, indicar las acciones preventivas y correctivas que se deban aplicar para asegurar la integridad de la información;

En virtud a lo expuesto en los párrafos precedentes, resulta necesario aprobar vía acto resolutivo el "Plan de Contingencia Informático" que tiene como objetivo establecer la organización y procedimiento a seguirse para garantizar la continuidad del procedimiento de la información ante pérdida o deterioro, permitiendo garantizar la operatividad de la empresa; así como, indicar las acciones preventivas y correctivas que se deba ejecutar para asegurar la integridad de la información de la empresa ante posibles desastres;

Con el visto de la Gerencia de Administración y Finanzas, Gerencia de Asesoría Jurídica, Oficina de Tecnología de la Información y Comunicaciones, y en uso de las facultades y atribuciones conferidas a este despacho a través del Estatuto Social de la empresa;



...RESOLUCIÓN DE GERENCIA GENERAL
N° 124-2023-GG-EPS.EMAPICA S.A.

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el **PLAN DE CONTINGENCIA INFORMÁTICO** de la EPS EMAPICA S.A., que consta con el siguiente contenido: I. Objetivos, II. Alcance, III. Plan Preventivo, IV. Organización para el Plan de Contingencia, V. Procesos y Procedimientos para el Plan de Contingencia, VI. Recursos e Infraestructura, VII. Determinación de la Localidad Alterna, VIII. Plan de Pruebas y Mantenimiento, y IX. Ejecución del Plan, la misma que se anexa y forma parte de la presente resolución.

ARTÍCULO SEGUNDO. – DISPONER que la Oficina de Tecnología de la Información y Comunicaciones y demás áreas involucradas, procedan a dar estricto cumplimiento al Plan de Contingencia Informático, que forma parte integrante de la presente resolución, a partir del día siguiente de su notificación.

ARTÍCULO TERCERO. – ENCARGAR a la Gerencia de Administración y Finanzas, el seguimiento del Plan que forma parte integrante de la presente resolución.

ARTÍCULO CUARTO.- DISPONER a la asistente administrativo de la Gerencia General, remitir la presente Resolución al presidente de la Comisión de Dirección Transitoria (CDT) de EPS EMAPICA S.A., para su conocimiento y fines competentes.

ARTÍCULO QUINTO.- DISPONER a la Oficina de Tecnología de la Información y Comunicaciones proceda a publicar la presente resolución en el Portal Institucional de la EPS EMAPICA S.A. (www.emapica.com.pe).

ARTÍCULO SEXTO.- NOTIFICAR la presente resolución y su anexo a las Gerencias de Línea, de Apoyo y Asesoría, Administraciones Zonales, Oficinas, y demás instancias competentes interesadas.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE




ING. RAÚL ADOLFO LINARES MANCHEGO
GERENTE GENERAL
EPS EMAPICA S.A.



Empresa Municipal de Agua Potable y Alcantarillado de Ica.

Plan de contingencia Informático

Oficina de Tecnología de la Información y Comunicaciones

2023



INDICE

1. Objetivos
2. Alcance
3. Plan Preventivo
 - 3.1. Integridad de datos.
 - 3.2. Identificación de usuarios
 - 3.3. Control de accesos a ambientes físicos
 - 3.4. Confidencialidad de datos
4. Organización para el Plan de Contingencia
 - 4.1. Roles y responsabilidades
5. Procesos y procedimientos para el Plan de Contingencia
 - 5.1. Procesos Críticos
 - 5.2. Responsables
6. Recursos e Infraestructura
 - 6.1. Recursos Humanos
 - 6.2. Suministros
 - 6.3. Energía Eléctrica
 - 6.3.1. Equipos
7. Determinación de la localidad alterna
8. Plan de pruebas y mantenimiento
 - 8.1. Generalidades de la prueba
 - 8.2. Recursos.
 - 8.3. Actividades
9. Ejecución del Plan



PLAN DE CONTINGENCIA INFORMATICO

1. Objetivos

- 1.1. Establecer la organización, normas y procedimientos a seguirse para garantizar la continuidad del procedimiento de la información, ante pérdida o deterioro, permitiendo garantizar la operatividad de la empresa.
- 1.2. Indicar las acciones preventivas y correctivas que se deban ejecutar para asegurar la integridad de la información, la vida humana y equipos de la empresa, ante posibles causas como:

Desastres:

Terremotos
Inundaciones
Incendios
Fallas de Energía prolongadas
Violencia (Explosiones, Robos, etc.)
Otros

Emergencias y/o Menores:

Huelgas
Fallas de Operación de la Red
Fallas de Programación
Virus Informáticos
Fallas o Falta de Energía

2. Alcance

Todo el personal de la EPS EMAPICA S.A. involucrado en el tratamiento de la información.

3. Plan Preventivo

3.1. Integridad de datos

Definirá acciones que protejan la información ante posibles fallas de energía eléctrica y/o equipos, ante desastres, manteniendo la integridad de los archivos y que no presenten corrupciones.

3.1.1. Generación de copias de respaldo

Tiene por objetivo garantizar la recuperación de la información en caso de pérdida total o parcial, diariamente al final de la jornada de trabajo se debe obtener una copia de los Archivos que se encuentran en el servidor de la Red.

Las copias deberán realizarse en un Unidad de almacenamiento en red My Cloud, 16TB, 2 Bahías GbE en una de las oficinas fuera de la Oficina de Tecnologías de la Información y comunicaciones o en el disco duro de una estación de trabajo; cada dos días la copia que se encuentra en la estación de trabajo deberá ser pasada a Unidad de almacenamiento en red My Cloud, 16TB, 2 Bahías GbE para su almacenamiento fuera del local institucional en un lugar protegido de polvo, humedad y sismos.

3.1.2. Protección contra Virus

Tiene por objetivo evitar la infección de la Red con virus informático, tomándose en cuenta las siguientes consideraciones:



- Solo los computadores de la EPS EMAPICA SA estarán bajo el dominio los equipos de entidades externas que requieran el uso de internet utilizaran el internet como invitados sin ingresar a nuestro dominio.
- Todo Archivo contenido en cd's, dvd's o memoria USB de procedencia externa deberá ser escaneado por el personal de la Oficina de Tecnología de la Información y Comunicaciones con antivirus antes de ser copiada su información al servidor de la Red.
- Las estaciones de trabajo deberán contar necesariamente con antivirus residentes.
- Los antivirus deberán ser actualizados cada vez que sale una nueva versión.

3.2. Identificación de Usuarios

3.2.1. Generación de Usuarios y Privilegios

Tiene por finalidad establecer claramente quienes son aquellas personas que tienen acceso a la Red, así como especificar también a que discos lógicos, directorios, aplicativos, tendrán acceso y en que niveles.

3.2.2. Generación y Mantenimiento de Passwords

Tiene por finalidad asegurarse de que la persona que accesa a la Red, es aquella que fue autorizada. El mantenimiento del password evita que por el uso constante del mismo este pueda ser descubierto y utilizado inapropiadamente por una persona no autorizada.

3.3. Control de Accesos a Ambientes Físicos

3.3.1. Formas de Acceso a Ambientes Físicos

Solo el personal de la Oficina de Tecnología de la Información y Comunicaciones tendrá acceso a la misma; las demás personas requerirán la autorización de la Gerencia General para su ingreso a la Oficina. Esto tiene como objetivo asegurar la integridad física del servidor de la Red y el Concentrador de la Red.

3.3.2. Alarmas en Ambientes Físicos

Es necesario considerar alarmas como prevención frente a cualquier contingencia no prevista. Como un detector de Humo, grifos contra incendio

3.4. Confidencialidad de Datos

3.4.1. Generación de Encriptación de Datos

Las aplicaciones que se desarrollen deberán manejar para aquellos archivos o datos que se consideren críticos, métodos de encriptación a fin de evitar que usuarios no autorizados puedan efectuar lecturas y/o modificaciones en las bases de datos

4. Organización para el Plan de Contingencia Informático

4.1. Roles y Responsabilidades

Responsables de la Ejecución del Plan

- Gerente General: Ing. Raúl Adolfo Linares Manchego
Dirección:
Celular Trabajo: 975375998
Celular Personal: 953646443
- Jefe de Tecnología de la Información y Comunicaciones: Ing. Victor Gutierrez Chauca
Dirección: Jr. Alfonso Ugarte N° 363 - Parcona - Ica
Teléfono Casa: 056-253184
Celular Trabajo: 945252055



Celular Personal: 979107040

- Administrador de la Red: Tec. Javier Leonel Retamozo Roque
Dirección: La Máquina A-40 La Tinguíña - Ica
Teléfono:
Celular Personal: 967304145

Responsabilidades

Del Gerente General:

- Brindar el apoyo mediante coordinaciones del nivel que le compete (Convenios, solicitudes de apoyo externo, etc.).
- Supervisar en coordinación con el Jefe de la Oficina de Tecnología de la Información y Comunicaciones la Ejecución del Plan.
- Ordenar el Apoyo Logístico necesario para la ejecución del Plan.

Del Jefe de la Oficina de Tecnología de la Información y Comunicaciones:

- Dirección Técnica de la Ejecución del Plan.
- Coordinación con la Gerencia General, áreas usuarias y el personal bajo su responsabilidad.
- Brindar Apoyo Técnico Operativo.
- Coordinar y mantener actualizado el Plan de Contingencia Informático.

Del Administrador de la Red:

- Apoyo total en la Ejecución del Plan
- Dirección del Plan en lo "Contingencias Menores"
- Coordinar con la Jefatura de Centro de Computo los requerimientos mínimos y los detalles concernientes a la Ejecución del Plan.
- Coordinar el Apoyo Logístico.
- Mantener al día los backups del Sistema, de los aplicativos y otros. Llevar al día la documentación de éstos.

5. Procesos y Procedimientos para el Plan de Contingencia Informático.

Tiene como objetivo identificar aquellos procesos que sin los cuales la empresa no podría operar y que tienen prioridad para ser restaurados en caso de pérdida de información.

5.1. Procesos Críticos

5.1.1. ESIINCO WEB

Los módulos son:

- Reglas de negocio
- Solicitud y Presupuesto
- Catastro
- Medición
- Facturación
- Cartera Morosa
- Micromedición
- Cobranza
- Reclamos
- Cierres y Aperturas
- Reclamos Online
- Sunass
- Consulta
- Adicionales
- VMA
- Dispositivos móviles
- Indicadores de gestión comercial



- Reportes Estándar
- Bancos
- Sunat

5.1.2. AVALON

Los módulos son:

- Patrimonio
- Contabilidad
- Recursos Financieros
- Recursos Humanos
- Suministros
- Logística
- Planeamiento

5.1.3. STD Sistema de Trámite Documentario

5.1.4. SGIO Sistema de Incidencias Operativas

5.1.5. MESA DE PUERTAS VIRTUAL

5.1.6. SICAP

5.1.7. SIAF

5.1.8. ESCADA

5.1.9. VIDEOVIGILANCIA

5.1.10. PCM TRANSPARENCIA

5.1.11. SISTEMA DE RADIO COMUNICACIONES

5.2. Responsables

<u>Proceso</u>	<u>Dueño</u>
ESIINCO WEB	Gerente Comercial
AVALON	Gerente Administración y Finanzas
STD Sistema de Trámite Documentario	Gerente Administración y Finanzas
SGIO Sistema de Incidencias Operativas	Gerente de Operaciones
Mesa De Partes Virtual	OTIC
SICAP	OTIC
SIAF	Gerente Administración y Finanzas
Escada	Gerente de Operaciones
Videovigilancia	OTIC
PCM Transparencia	OTIC
Sistema De Radio Comunicaciones	OTIC

6. Recursos e Infraestructura

6.1 Recursos Humanos

Los recursos humanos a utilizarse estarán constituidos por el personal de la Oficina de Tecnología de la Información y Comunicaciones y el dueño del proceso.

6.2 Suministros



Los suministros básicos a emplearse serán aquellos dispositivos de almacenamiento en los que se contengan las copias de respaldo.

6.3 Energía Eléctrica

Se contará como fuente de suministro de energía eléctrica a las fuentes convencionales de electricidad y también se cuenta con un sistema de respaldo de energía que garantiza la continuidad del negocio en cortes prolongados de energía eléctrica compuesto por los siguientes equipos:

- Grupo electrógeno de potencia 20KW/25KVA.
- UPS 20 KVA + 02 transformadores de aislamiento DE 25 KVA 220V/380V Y 380V/220V + caja protección de UPS.

6.4 Equipos

Se deberá considerar la posibilidad de utilizar otro computador de la EPS como servidor o en su defecto la posibilidad de obtener otro de fuente externa; también es necesario determinar que estaciones de trabajo puedan remplazar a las que se encuentran en los puntos críticos.

7 Determinación de una Localidad Alterna.

La EPS buscará una empresa o Institución con sistemas de cómputo análogos para crear convenios de apoyo que estas se conviertan en centros alternos de procesamiento para el lapso que dure la contingencia.

Los aspectos principales a tomar en cuenta son:

- Sistema Operativo de la red local
- Software base
- Capacidad de almacenamiento
- Estaciones de trabajo

8 Plan de Pruebas y Mantenimiento

Tiene por objetivo probar que el Plan de Contingencias funciona, pues "Probar es convertir el Plan de Contingencias de la Empresa, de un concepto planeado a una realidad"

8.1 Generalidades de la Prueba

La prueba simulará una "Caída" total del servidor de la Red y algunos periféricos, de tal manera que en nuestro desastre supuesto quedarán inutilizados los siguientes equipos:

- Servidor de Red
- Estaciones de Facturación
- Estaciones de Cobranzas
- Estaciones de Contabilidad
- Se verificará que el tiempo de los procesos está dentro de lo esperado por el área usuaria.

8.2 Recursos

- Para ejecutar la prueba se deberá seleccionar aquellos computadores que tengan las características más similares posibles a los computadores supuestamente inutilizados.
- Se contará con los dispositivos de almacenamiento de las copias de respaldo; es decir disco duro de una estación de trabajo o Unidad de almacenamiento en red My Cloud, 16TB, 2 Bahías GbE, cd's o dvd's.

8.3 Actividades

- Anotación de tiempos de inicio y final de la prueba
- Instalación del Servidor Windows 2022.
- Conexión de Estaciones de Trabajo
- Instalación del Software, aplicativos y bases de datos
- Estimación del tiempo de digitación de la data supuestamente perdida
- Prueba que lo instalado funciona



- Conclusiones y Recomendaciones para mejorar/actualizar el Plan
- Generar un documento con el resultado de la prueba.

9. Ejecución del Plan de Contingencias Informático.

De contingencias menores:

- Comunicación inmediata al Jefe o Auxiliar de la Oficina de Tecnología de la Información y Comunicaciones.
- Se identificará la emergencia y luego los procesos y archivos críticos que sean afectados
- El auxiliar de la Oficina de Tecnología de la Información y Comunicaciones adoptará las decisiones para el uso de recursos internos y de backups.
- Se realizará un informe para que en lo posible se corrija.y/o eviten determinantes.

De contingencias mayores:

- Comunicación inmediata al Jefe de Oficina de Oficina de Tecnología de la Información y Comunicaciones.
- El Jefe de la Oficina Oficina de Tecnología de la Información y Comunicaciones tomará la dirección del Plan de Contingencias y se procederá a hacer uso de la "Instalación del Sistema Alternativo"
- El Jefe de la Oficina de Oficina de Tecnología de la Información y Comunicaciones identificará el problema y realizará una evaluación de la magnitud de la Contingencia.
- Se adoptará todas las medidas de seguridad en emergencias.
- Una vez superada la emergencia se evacuará un informe para luego proceder a una recuperación local.

