PLAN DE CONTINGENCIA INFORMÁTICO DE LA EMPRESA MUNICIPAL ADMINISTRADORA DE PEAJE DE LIMA

Versión: 02	Código: GAF-SGTI-004-2014	Fecha: Abril de 2014	Nº Páginas: 33

Rubro	Nombre	Cargo	Firma
REVISADO POR	DANTE ANTIPORTA POMACAJA	SUB GERENTE DE TECNOLOGÍA DE INFORMACIÓN	MUNICIPALIDAD METROPOLITANA DE LIMA Empresa Municipal Administradora de Peaje de Lima S.A. Ing. Dante Antiporta Pomacaja SUB GERENTE DE TECNOLOGÍA DE INFORMACIÓN
APROBADO POR	JOSE ANTONIO LEÓN AMBIA	GERENTE DE ADMINISTACIÓN Y FINANZAS	MUNICIPALIDAD METROPOLITANA DE LIMA Empresa Municipal Administradora de Peaje de Lima S.A. José Antonio León Ambia Gerente de Administración y Finanzas

INDICE

I. INTRODUCCIÓN

El Plan de Contingencia podemos definirlo como el conjunto de procedimientos alternativos a la operatividad de la Institución, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo debido a algún incidente, desastre o sabotaje tanto interno como ajeno a la Institución. Las causas son variadas y pasan desde un problema informático, un fallo en energía eléctrica, telecomunicaciones, hasta desastres naturales o sabotajes

El Plan de Contingencia no implica un reconocimiento de la ineficiencia sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas anteriormente que pueden provocar importantes pérdidas, no solo materiales sino de la información Institucional, y de aquellas derivadas de la paralización de las funciones de la Empresa Municipal Administradora de Peaje de Lima S.A (EMAPE) durante un periodo más o menos prolongado.

El presente documento pretende ayudar a comprender mejor la problemática del entorno informático, ya que toda la institución debe estar preparada para el caso de ocurrencias imprevistas

II. OBJETIVO

El principal objetivo de un Plan de Contingencia es plasmar las acciones necesarias para garantizar la continuidad de las operaciones de la Empresa Municipal Administradora de Peaje de Lima (EMAPE S.A.)

La alta dirección debe tomar conciencia que el desarrollo y la implementación de planes de contingencia comprende a toda la Institución, pues se trata de una situación de continuidad de las funciones de EMAPE y no puramente de la Gerencia de Administración y Finanzas o de la Sub Gerencia de Tecnología de Información.

III. FINALIDAD

El referido Plan tiene como finalidad identificar los riesgos, establecer los procedimientos y los mecanismos para preservar la seguridad de los equipos de cómputo, proteger la información almacenada en ellos, y garantizar la continuidad de las funciones de la Empresa Municipal Administradora de Peaje de Lima.

IV. ALCANCE

Están comprendidos en la ejecución del presente plan los funcionarios, directivos, personal encargado del equipo de informática y los responsables de cada gerencia de las oficinas de la Sede Central de EMAPE S.A. y como conocimiento general, a todos los trabajadores.

V. BASE LEGAL

- La Ley de la Actividad Empresarial del Estado N° 24948; y su Reglamento Decreto Supremo N° 027-90-MIPRE.
- Constitución Política del Estado, Artículo 192°, inciso 4), dispone que las Municipalidades, en ejercicio de su autonomía política, económica y administrativa, tienen competencia exclusiva para organizar, reglamentar y administrar los servicios públicos de su circunscripción

- Ley 27972 – Ley Orgánica de Municipalidades, publicada el 27 de Mayo del 2003 (Artículos 35°, 69° Inciso 11, 157° Inciso 13, 161° Inciso 1, numeral 1.1. Inciso 7, numeral 7.3. y 166° Inciso 2), y sus modificatorias.
- La Ley General de Sociedades N° 26887 publicada el 09 de diciembre de 1997
- Ley Orgánica de Municipalidades Ley N° 27972.
- Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 29091 – Normas Legales.
- Decreto Supremo N° 063-2010-PCM
- Resolución Ministerial N°200-2010.

VI. DISPOSICIONES GENERALES

1. ANÁLISIS DE RIESGO

Este proceso en general consiste, en la identificación de amenazas, las que en combinación con un análisis de frecuencia y consecuencias permiten estimar un riesgo.

Objetivos:

- Identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar las condiciones operativas de la red de cómputo institucional
- Establecer, con fundamento en el análisis de riesgo, las bases para la preparación del Plan de Contingencia del riesgo estimado.

1.1 Identificación de Actividades que Implican Riesgos

Los lugares principales de ocurrencia de una emergencia son las diversas Gerencias, Sub Gerencias u Oficinas de EMAPE S.A.

Al evaluar la probabilidad de ocurrencia de un evento se asignará un valor único para la dependencia, sin embargo es importante establecer diferencias según el ***Grado de Vulnerabilidad*** que presenten las áreas a intervenir. Por ejemplo, el corte de fluido eléctrico combinado con un incendio, representa mayores riesgos de pérdida de información que la inoperatividad de las computadoras por desfase tecnológico

1.2 Identificación de Amenazas

Una amenaza se define como el evento de posible ocurrencia con capacidad de afectar negativamente las instalaciones y actividades de EMAPE S.A. y consecuentemente su imagen.

Aquellos eventos negativos que puedan afectar el desarrollo normal de las actividades que se ejecutan en las Gerencias de EMAPE S.A., se conocen como amenazas de tipo **endógenas** y requieren de un plan de contingencia para su prevención y atención, entre ellas se consideran: Problemas con la tubería de agua y desagüe, inconvenientes eléctricos, cableado de red dañado, etc.

Por otra parte, el desarrollo de actividades ajenas al tema informático sumadas a los fenómenos naturales puede llegar a constituirse en elementos perturbadores del medio ambiente y posibles generadores de emergencias. Estas **amenazas** son de tipo **exógeno** y entre ellas se consideran: Incendios, sismos, atentados y robo.

Las amenazas que podrían afectar las instalaciones de EMAPE S.A. y sus posibles causas se explican a continuación:

1.2.1 Factores Endógenos

1.2.1.1 Problemas con la tubería de Agua y Desagüe

No ocurren frecuentemente en los ambientes de las diversas Gerencias de EMAPE S.A., pero en el caso que se llegara a dar, los daños que causarían serían cuantiosos. Su ocurrencia puede deberse principalmente a la negligencia de los empleados, debido a la disposición de las tuberías de agua y la proximidad de los servicios higiénicos a las oficinas. El peligro de afectación de equipos puede llevarse a cabo en forma horizontal (en el mismo piso). A esto se agrega el peligro de que la gran mayoría de computadoras no cuenten con fundas impermeables que minimicen estos inconvenientes.

1.2.1.2 Daño del Cableado de Red

Para que los equipos informáticos de EMAPE S.A se integren a una red de cómputo y accedan a sus servicios, se usan cables de cobre en algunos casos, los mismos que se encuentran protegidos por canaletas plásticas (ya sea de pared o de piso) y en el resto de los casos la conexión y el acceso es vía inalámbrica (Wireless). La presencia de esta amenaza se circunscribe desde la inaccesibilidad a la red por parte de un equipo, pasando por la de una Gerencia, todo un piso y en el caso más grave a toda la sede central de EMAPE S.A. y locales anexos, todo ello provocado por cortes de cable, quiebres de cable, estiramientos de cable, amalgamientos con cables eléctricos y/o telefónicos, sulfatación de conectores entre otros factores; o en los casos de conexiones inalámbricas, puede ser ruidos, vibraciones, interferencias, entre otros.

PISO	PUNTOS DE RED INTALADOS
PISO 1	13
UBICACIÓN	**ACCESS POINT**
OPERACIONES	1
TECNOLOGIA DE INFORMACIÓN	2
ESTUDIOS Y PROYECTOS	3
MANTENIMIENTO	1
INFRAESTRUCTURA	1
PLANIFICACIÓN Y PRESUPUESTO	1
LOGISTICA	1
ADMINISTRACIÓN Y FINANZAS	1
ASUNTOS LEGALES	1
DIRECTORIO	1

Esquema de red de EMAPE (plano de red)

1.2.1.3 Fallas de Equipo de Comunicaciones

La Red de cómputo llega a todas las Gerencias de EMAPE S.A. a través de los equipos de comunicaciones (ya sean Switches o Access Points) ubicados estratégicamente en los sectores norte, centro y sur de las instalaciones, tal como se detalla seguidamente.

PISO	N° Access Point	N° Routers	N° Switchs	DEPENDENCIA
1s	1			DIRECTORIO
			1	IMAGEN INSTITUCIONAL
	1			GERENCIA DE ASUNTOS LEGALES
1c			17	GERENCIA DE ADMINISTRACIÓN Y FINANZAS
	2			LOGISTICA
	2	3	1	TECNOLOGIA DE INFORMACIÓN
	1			GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO
1n	1			GERENCIA DE INFRAESTRUCTURA
	1		1	MANTENIMIENTO
	3		2	GERENCIA DE ESTUDIOS Y PROYECTOS
	1		1	GERENCIA DE OPERACIONES
TOTAL	13	3	23	

Donde: n = sector norte, c = sector central y s = sector sur

Obviamente la alteración y/o inoperatividad de algunos de estos componentes se traducirían en que determinadas Gerencias no tengan acceso a los servicios que brinda la red de EMAPE S.A.

1.2.1.4 Inoperatividad de Servidores de Comunicación

Es una situación fortuita, ocasionada por fallas de hardware y/o software, que acarrea la imposibilidad de acceder a los servicios de Internet tan común en nuestros días como: correo electrónico, navegación por páginas web, portales, transferencia de archivos (ftp), entre otros. Así mismo la imposibilidad de acceder a los servicios de la Intranet Institucional: OPERACIONES (Mantenimiento de afiliados, Clientes PostPago, Control de Exonerados, Registro de Ocurrencias); RECURSOS HUMANOS (Bienestar, Planillas, Asistencia Planillas, Asistencia SNP, Planilla Obreros), GENERAL (Gestión de la Calidad, Registro de Quejas y Sugerencias, Registro de actividades oficiales, Requerimientos de Bienes y Servicios, Solicitud de Honorarios, Generación de TXT COA Estado, Solicitud de Vehículos), documentos varios, entre otros.

1.2.1.5 Inoperatividad de Servidores de Base de Datos

Todos los Aplicativos y Sistemas de Información que almacenan sus datos en este Servidor estarían impedidos de acceder a su información (nivel interno), así como las aplicaciones que interactúan con el Portal de Internet no podrían brindar consultas de tipo "on line" en el ambiente de EMAPE S.A. virtual (nivel externo).

1.2.1.6 Inoperatividad del Servidor DNS Interno

Se cuenta con un Servidor DNS propiedad de EMAPE S.A. que resuelve los nombres de dominios internos, cuya falla originaría también problemas en la red.

1.2.1.7 Inoperatividad del Servidor de Correo

Se cuenta con un Servidor de correo por la cual circula todos los servicios de mensajería, cuya falla originaria la detención de los servicios de envío y recepción de mensajes a través del correo corporativo, a correos de diferentes dominios.

1.2.1.8 Inoperatividad del Servidor de Asistencias

Se cuenta con un Servidor de Asistencias que almacena el registro de Asistencias, cuya falla originaría la detención de los registros de asistencia de los trabajadores a la Empresa EMAPE S.A.

1.2.1.9 Inoperatividad del Servidor de Archivos

Se cuenta con un Servidor de Archivos que permite compartir y acceder a la información de acuerdo a las diferentes Áreas y Gerencias de EMAPE S.A., cuya falla originaría problemas con el acceso a los archivos disponibles en este Servidor.

1.2.1.10 Inoperatividad del Servidor de Directorio Activo

Se cuenta con un Servidor de Directorio Activo (Active Directory) que permite la gestión centralizada de equipos, usuarios y grupos, la cual gestiona entre otras cosas los inicio de sesión y las políticas de acceso a los usuarios que laboran en la empresa, cuya falla originaría que los usuarios no puedan acceder a la red interna.

1.2.1.11 Inoperatividad del Servidor de Intranet

Se cuenta con un Servidor de Intranet que permite la gestión de sistemas web e Intranet del portal electrónico, la cual gestiona entre otras cosas los servicios de la intranet, cuya falla originaría que los usuarios no puedan acceder al sistema web de EMAPE S.A. por consiguiente el portal electrónico

1.2.1.12 Inconvenientes Eléctricos

Por razones de seguridad interna la Gerencia de Administración y Finanzas (GAF) debe disponer la supervisión y mantenimiento periódico de las instalaciones, dispositivos y conexiones de la red eléctrica de computo (tableros, circuitos, pozo a tierra, grupo electrógeno, entre otros).

1.2.1.13 Pérdida de Información

Que afectaría lo dispuesto en la "Ley de Transparencia" la cual establece la publicación de la información concerniente a EMAPE S.A. utilizando la Intranet y el Portal Institucional para el acceso del público en general.

Mención especial merece el tema del almacenamiento físico de los medios donde se realizan las copias de seguridad en los Servidores de Backup y un Disco Duro Externo, medida importante para evitar la pérdida de información, los cuales hasta el momento son custodiadas por la Oficina de Soporte Tecnológico.

La información del usuario que está almacenada en el disco duro de la computadora de trabajo, es total responsabilidad de cada trabajador, Jefe y/o Gerencia.

1.2.1.14 Acción de Virus Informático

Se consideran a los virus informáticos como amenazas endógenas cuando se infiltran desde el interior de la Institución a través del uso de diskettes, memorias USB, discos externos, discos compactos, mala manipulación y mal uso de descargas a través de internet por parte del usuario, uso de cualquier otro dispositivo de almacenamiento infectados por parte de los usuarios de EMAPE S.A y como amenazas exógenas cuando se infiltran a través del correo electrónico y la navegación en internet.

Es importante señalar que las computadoras de la Institución cuentan con el Servicio de Antivirus, el cual es actualizado periódicamente

1.2.1.15 Alteración del Información

Los diversos aplicativos y Sistemas de Información implementados en la red de EMAPE S.A. son accedidos a través del software instalado en la computadora cliente, con los niveles de acceso y/o capas de seguridad que provee dicho software, el Motor de Base de Datos y la plataforma operativa. Hay que indicar que los usuarios que accesan a las diferentes fuentes de información son personal autorizado formalmente por su jefe inmediato o Gerente. Esto garantiza el acceso a la información sólo al personal autorizado, evitando su manipulación por personal no autorizado que traería como consecuencia graves daños a la información.

La administración de la instalación en donde se ubican los servicios de EMAPE S.A. está a cargo de la Sub Gerencia de Tecnología de Información de la Gerencia de Administración y Finanzas, a través de la Oficina de Soporte Tecnológico.

1.2.2 Factores Exógenos

1.2.2.1 Corte de Fluido Eléctrico

Todos los equipos informáticos usan la electricidad por lo que su ausencia conduce directamente a una inoperatividad de los mismos.

1.2.2.2 Corte de Servicio de Circuito Digital

EMAPE S.A. cuenta con un circuito digital para transmisión / recepción de datos con un ancho de banda de 20 Mbps. Un corte temporal o definitivo de este tipo de servicio "aislaría" tecnológicamente a la Institución a nivel nacional e internacional.

1.2.2.3 Averías del Circuito Digital

Este tipo de conexión tiene un tramo físico fuera de la sede institucional, susceptible de presentar averías y por ende degradación de los servicios que hacen uso de dicho tipo de conexión. Tal son los casos de inconvenientes ocasionados al circuito por parte de las empresas proveedoras de agua, electricidad, cable y otros, que al efectuar trabajos de campo pueden dañar las líneas de transmisión del circuito digital u otros factores que pueden interferir con la señal inalámbrica.

1.2.2.4 Inoperatividad del Servidor DNS Externo

El servidor DNS que resuelven los nombres de dominios de Internet está bajo la administración de la Oficina de Soporte Tecnológico de la Sub Gerencia de Tecnología de Información de la Gerencia de Administración y Finanzas, en este caso, cuya inoperatividad se traduciría en la imposibilidad de acceder a Internet

1.2.2.5 Acción de Virus Informáticos

Se consideran los virus informáticos como amenazas exógenas debido a que pueden alterar el normal desenvolvimiento de las actividades, infiltrándose desde el exterior a través del correo electrónico, archivos adjuntos infectados o con la acción de navegar en Internet. Es de suma importancia señalar que los usuarios de la red, cuentan con el servicio de actualización automática del Software Antivirus y protección adicional a nivel de servidor de correo

1.2.2.6 Incendios

Se debería contar con una Oficina de Defensa Nacional en virtud a lo establecido en el Plan de Trabajo Institucional, capacitado e instruyendo periódicamente a los Brigadistas designados en cada dependencia de la Institución en el uso de extintores con carga de producto de dióxido de carbono y gas Halon 1211 los cuales son utilizados para la protección exclusiva de los equipos de cómputo. Asimismo se deberá capacitar en el uso de extintores ABC, para ser utilizados en la preservación de las instalaciones de la Sede Central.

La institución no cuenta con sistemas detectores de humo ni de aspersión automática en la Sala de Servidores y Comunicaciones.

La Oficina de Defensa Nacional (En caso de existir) debería periódicamente preparar charlas de capacitación dirigidas a todo el personal de EMAPE para que se pueda enfrentar a cualquier tipo de desastre.

1.2.2.7 Sismos

Las oficinas de EMAPE S.A., no se encuentran en un edificio que cumpla con las normas técnicas antisísmicas, por lo que los daños que podrían causar al parque informático serían de tipo moderado.

1.2.2.8 Atentados

Son actos criminales efectuados por personas o grupos al margen de la ley EMAPE S.A., cuenta con personal de seguridad, quienes se encuentran ubicados estratégicamente en las diversas áreas y puertas de acceso de la Sede Central, para realizar labores de control y vigilancia a efectos de evitar cualquier robo de diversa naturaleza.

Adicionalmente, se estima conveniente que la empresa de seguridad que presta sus servicios en la sede Central, garantice la honestidad y honradez de los agentes de servicio de vigilancia, a fin de evitar que estos resulten involucrados en acciones deshonestas.

1.2.2.9 Hackers

Si entendemos como Hacker al individuo que usa sus habilidades y recursos para invadir sistemas informáticos ajenos, se entiende que estamos expuestos a este tipo de accesos que pueden ocasionar daños en la red de EMAPE S.A. Se debe mencionar que la red de la empresa no cuenta con un Sistema de Prevención de Intrusos (IPS), por ello el control de accesos a la red se gestiona vía la MAC de la tarjeta de red. La red de EMAPE S.A si cuenta con un Firewall – basado en software – que controla los accesos

Finalmente es conveniente realizar en la Sede Central de EMAPE S.A., un resumen de riesgos ordenados por el factor de riesgo cada uno.

1.3 Definición de Posibles Escenarios

Un escenario es la combinación de una amenaza con una actividad, y se define como la posibilidad para que una amenaza determinada se materialice como una emergencia en un sitio determinado

La definición de escenarios se hará combinando las actividades y amenazas identificadas en los numerales anteriores. Los resultados de esa combinación se presentan en la **Tabla 02.**

Tabla N° 02 - Escenarios de Emergencia

		Amenazas	Actividad	
			Internet	Base de Datos y Sistemas
Endógenos	1	Problemas con la tubería de agua y desagüe	X	X
	2	Diseño de cableado de red	X	X
	3	Fallas de Equipos de Comunicación	X	X
	4	Inoperatividad de Servidores de Comunicación	X	
	5	Inoperatividad de Servidores de Base de Datos		X
	6	Inoperatividad del Servidor DNS Interno	X	
	7	Inoperatividad del Servidor de Correo	X	
	8	Inoperatividad del Servidor de Asistencias	X	
	9	Inoperatividad del Servidor de Archivos	X	
	10	Inoperatividad del Servidor de Directorio Activo	X	
	11	Inoperatividad del Servidor de Intranet	X	
	12	Inconvenientes Eléctricos	X	X
	13	Pérdida de Información		X
	14	Acción de Virus		X
	15	Alteración de la Información		X
	16	Corte de Fluido Eléctrico	X	X
	17	Corte de Servicio de Circuito Digital	X	
	18	Averías del Circuito Digital	X	
Exógenos	19	Inoperatividad del Servidor DNS Externo	X	
	20	Acción de Virus		X
	21	Incendios	X	X
	22	Sismos	X	X
	23	Atentados	X	X
	24	Hackers		X

Internet	Acceso a herramientas: e-mail, ftp, browser, base de datos, intranet.
Base de Datos / Sistemas	Administración, desarrollo, ingreso de datos, administración de file servers.

TABLA N° 03 - Probabilidad de los Siniestros

Probabilidad	Definición	Ocurrencia de Eventos	Puntaje
Frecuente	De ocurrencia Alta	1 al mes	6
Moderado	De ocurrencia Media	Entre 2 y 6 meses	5
Ocasional	De ocurrencia Limitada	Entre 7 y 12 meses	4
Remoto	De ocurrencia Baja	Entre 1 y 5 años	3
Improbable	De ocurrencia muy Baja	Entre 6 y 10 años	2
Imposible	Excepcional posibilidad de ocurrencia	De 10 años a más	1

La probabilidad de ocurrencia se define en la **Tabla 03** asignado a cada clase un puntaje numérico.

Tabla N° 04 - Estimación de Probabilidades

		Amenazas	Actividad	
			Probabilidad	Puntaje
Endógenos	1	Problemas con la tubería de agua y desagüe en la actividad de Internet	Ocasional	4
	2	Problemas con la tubería de agua y desagüe en la actividad de Base de Datos	Ocasional	4
	3	Daño del Cableado de Red en la actividad de internet	Moderado	5
	4	Daño del Cableado de Red en la actividad de Base de Datos	Moderado	5
	5	Falla de equipos de Comunicación en la actividad de internet	Ocasional	4
	6	Falla de equipos de Comunicación en la actividad de Base de Datos	Ocasional	4
	7	Inoperatividad de Servidores de Comunicación en la actividad de Internet	Ocasional	4
	8	Inoperatividad de Servidores de Base de Datos en la actividad de Sistemas	Ocasional	4
	9	Inoperatividad del Servidor DNS Interno en la actividad de internet	Improbable	2
	10	Inoperatividad del Servidor de Correo	Ocasional	4
	11	Inoperatividad del Servidor de Asistencias	Ocasional	4
	12	Inoperatividad del Servidor de Archivos	Ocasional	4
	13	Inoperatividad del Servidor de Directorio Activo	Ocasional	4
	14	Inoperatividad del Servidor de Intranet	Ocasional	4
	15	Inconvenientes eléctricos en la actividad del Internet	Moderado	5
	16	Inconvenientes eléctricos en la actividad de Base de Datos - Sistemas	Moderado	5
	17	Pérdida de Información en la Actividad de Base de Datos	Remoto	3
	18	Acción de Virus en la actividad de Internet	Remoto	3
	19	Acción de Virus en la actividad de Base de Datos - Internet	Remoto	3
	20	Alteración de la Información en la actividad de Base de Datos	Improbable	2
Exógenos	1	Corte de Fluido Eléctrico en la actividad de Internet	Ocasional	4
	2	Corte de Fluido Eléctrico en la actividad de Sistemas	Ocasional	4
	3	Corte del servicio de Circuito Digital en la actividad de Internet	Improbable	2
	4	Averías en el Circuito Digital en la actividad de Internet	Improbable	2
	5	Inoperatividad del Servidor DNS Externo en la actividad de internet	Improbable	2
	6	Acción del Virus en la actividad de sistemas	Ocasional	4
	7	Incendios en la actividad de Internet	Improbable	2
	8	Incendios en la actividad de Sistemas	Improbable	2
	9	Sismos durante la actividad de Internet	Ocasional	4
	10	Sismos durante la actividad de Sistemas	Ocasional	4
	11	Atentados en la actividad de Internet	Imposible	1
	12	Atentados en la actividad de Sistemas	Imposible	1
	13	Ataque de hackers	Ocasional	4

1.3.1 Definición de Factores de Vulnerabilidad

La vulnerabilidad es el grado relativo de sensibilidad, que un sistema tiene respecto a una amenaza determinada. Los factores de vulnerabilidad dentro de un análisis de riesgos, permite determinar cuáles son los efectos negativos, que sobre un escenario y sus zonas de posible impacto pueden tener los eventos que se presenten. Para efectos del análisis de riesgo, se consideran los siguientes factores de vulnerabilidad.

- **Victimas:** Se refiere al número y clase de afectados (empleados, personal de emergencia y la comunidad); considera también el tipo y la gravedad de las lesiones.
- **Daño ambiental:** Incluye los impactos sobre el aire y la comunidad a consecuencia de la emergencia.
- **Pérdidas materiales o económicas:** Representadas en instalaciones, equipos, productos, valor de las operaciones de emergencia, multas, indemnizaciones, y atención médica entre otros.
- **Imagen Institucional:** Califica el nivel de deterioro de la imagen de la Institución como consecuencia de la emergencia.
- **Suspensiones:** Determina los efectos de la emergencia sobre el desarrollo normal de las actividades de la Institución en términos de días perdidos.

1.3.2 Estimación de Gravedad

La gravedad de las consecuencias de un evento se evalúa sobre los factores de vulnerabilidad, y se califica dentro de una escala que establece cuatro niveles. Los niveles corresponden a gravedad nivel 1 o insignificante, nivel 2 o marginal, nivel 3 o crítica, nivel 4 o catastrófica. Los criterios de calificación para los factores de vulnerabilidad se presentan en la **Tabla 05.**

Tabla N° 05 - Calificación de la Gravedad

Factor de Vulnerabilidad	Calificación de Gravedad			
	Insignificante 1	Marginal 2	Crítica 3	Catastrófica 4
Victimas	No hay lesiones o no se requiere atención hospitalaria	Lesiones leves que requieren atención	Lesiones con necesidad de hospitalización	Muertes
Daño Ambiental	No hay impactos ambientales significativos	Impactos Ambientales dentro del área del escenario	Impactos en las áreas aledañas al escenario	Impacto con consecuencias sobre la comunidad
Pérdidas Materiales Económicas	Menos de $1,000	Entre $1,000 y $5,000	Entre $5,000 y $10,000	De $10,000 a más
Suspensiones	No hay Suspensión	Suspensión de 1 día	Suspensión de 2 días	Suspensión 3 días a más

1.3.3 Calculo del Riesgo

El riesgo es producto de la combinación de dos factores: la probabilidad de ocurrencia de una amenaza y la gravedad de las consecuencias de la misma.

Matemáticamente el **riesgo (R)** puede expresarse como el producto de la probabilidad de **ocurrencia (P)** por la **gravedad (G).**

$$R = P \times G$$

En la **Tabla 06** se presenta un resumen de la aceptabilidad de riesgos según combinación de probabilidad de ocurrencia y la gravedad de un evento.

Aceptabilidad del Riesgo			Gravedad			
			Insignificante 1	Marginal 2	Crítica 3	Catastrófica 4
Probabilidad de los Siniestros	1	Imposible	a	a	t	i
	2	Improbable	a	t	t	i
	3	Remoto	a	t	i	i
	4	Ocasional	t	t	i	i
	5	Moderado	t	i	i	i
	6	Frecuente	t	i	i	i

Leyenda	
Aceptable	a
Tolerable	t
Inaceptable	i

1.3.4 Aceptabilidad

En cuanto a la **aceptabilidad a los riesgos**, los escenarios se clasifican como:

- **Aceptable:** Un escenario situado en esta región de la matriz significa que la combinación de probabilidad-gravedad no representa una amenaza significativa por lo que no amerita la inversión inmediata de recursos y no requiere una acción específica para la gestión sobre el factor de vulnerabilidad considerado en el escenario. Cuantitativamente representa riesgos con valores menores o iguales a tres puntos

- **Tolerable:** Un escenario situado en esta región de la matriz significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, éstas tienen una prioridad de segundo nivel. Cuantitativamente representa riesgos con valores entre cuatro y seis puntos.

- **Inaceptable:** Un escenario situado en esta región de la matriz significa que se requiere siempre desarrollar acciones prioritarias e inmediatas para su gestión, debido al alto impacto que tendrían sobre el sistema. Cuantitativamente representa valores de riesgo entre ocho y veinticuatro puntos.

Aceptabilidad del Riesgo		
Aceptable	Tolerable	Inaceptable

1.3.5 Niveles de Planeación

La aceptabilidad de riesgos está directamente relacionada con los niveles de planeación de contingencias requeridos específicamente para EMAPE S.A., de la siguiente manera:

- **No Plan:** Un escenario situado en esta región de la matriz, significa que la combinación de probabilidad-gravedad no representa una amenaza significativa; por tanto no se requiere la inversión especifica de recursos especiales, ya que los mecanismos de control de existentes en EMAPE S.A contrarrestan significativamente los efectos del riesgo identificado.

- **Plan General:** Un escenario situado en esta región de la matriz significa que, aunque debe diseñarse una respuesta para dichos casos, ésta debe ser sólo de carácter general.

- **Plan Detallado:** Un escenario situado en esta región de la matriz significa que se requiere siempre diseñar una respuesta detallada a las contingencias y que es preciso realizar inversiones particulares para cada uno de estos escenarios

Niveles de Planeación		
No Plan	Plan General	Plan Detallado

Los resultados de la estimación de gravedad y los resultados del cálculo de riesgo y la aceptabilidad de los riesgos para los escenarios de emergencia son presentados en la **Tabla 07**

Tabla N° 07 - Valores de Gravedad y Riesgo para los diferentes Factores de Vulnerabilidad

Escenario				Factores de Vulnerabilidad									
				Victimas		Daño Ambiental		Pérdidas Económicas		Imagen Institucional		Suspensión	
	Amenazas		Probab.	G	R	G	R	G	R	G	R	G	R
Endógenos	1	Problemas con la tubería de agua y desagüe en la actividad de Internet	4	1	4	2	8	1	4	1	4	2	8
	2	Problemas con la tubería de agua y desagüe en la actividad de Base de Datos	4	1	4	2	8	1	4	1	4	2	8
	3	Daño del Cableado de Red en la actividad de internet	5	1	5	1	5	1	5	1	5	1	5
	4	Daño del Cableado de Red en la actividad de Base de Datos	5	1	5	1	5	1	5	1	5	1	5
	5	Falla de equipos de Comunicación en la actividad de internet	4	1	4	1	4	2	8	4	16	1	4
	6	Falla de equipos de Comunicación en la actividad de Base de Datos	4	1	4	1	4	2	8	1	4	1	4
	7	Inoperatividad de Servidores de Comunicación en la actividad de Internet	4	1	4	1	4	2	8	4	16	1	4
	8	Inoperatividad de Servidores de Base de Datos en la actividad de Sistemas	4	1	4	1	4	2	8	1	4	1	4
	9	Inoperatividad del Servidor DNS Interno en la actividad de internet	2	1	2	1	2	2	4	4	8	1	2
	10	Inoperatividad del Servidor de Correo en la actividad de internet	3	1	3	1	3	3	9	2	6	2	6
	11	Inoperatividad del Servidor de Asistencias en la actividad de Base de Datos - Sistemas	3	1	3	1	3	3	9	2	6	2	6
	12	Inoperatividad del Servidor de Archivos de Base de Datos - Sistemas	5	1	5	1	5	3	15	2	6	3	15
	13	Inoperatividad del Servidor de Directorio Activo de Base de Datos - Sistemas	5	1	5	1	5	3	15	2	6	3	15
	14	Inoperatividad del Servidor de Intranet de Base de Datos - Sistemas	3	1	3	1	3	3	9	1	6	2	6
	15	Inconvenientes eléctricos en la actividad del Internet	5	1	5	1	5	2	10	2	10	1	5
	16	Inconvenientes eléctricos en la actividad de Base de Datos - Sistemas	5	1	5	1	5	2	10	1	5	1	5
	17	Pérdida de Información en la Actividad de Base de Datos	3	1	3	1	3	2	6	1	3	1	3
	18	Acción de Virus en la actividad de Internet	3	1	3	1	3	2	6	1	3	1	3
	19	Acción de Virus en la actividad de Base de Datos - Internet	3	1	3	1	3	2	6	1	3	2	6
	20	Alteración de la información en la actividad de Base de Datos	2	1	2	1	2	3	6	1	2	1	2
Exógenos	1	Corte del Fluido Eléctrico en la actividad de Internet	4	1	4	1	4	4	16	1	4	2	8

2	Corte de Fluido Eléctrico en la actividad de Sistemas	4	1	4	1	4	4	16	1	4	2	8
3	Corte del servicio de Circuito Digital en la actividad de Internet	2	1	2	1	2	2	4	4	8	1	2
4	Averías en el Circuito Digital en la actividad de Internet	2	1	2	1	2	2	4	4	8	1	2
5	Inoperatividad del Servidor DNS Externo en la actividad de internet	2	1	2	1	2	2	4	4	8	1	2
6	Acción del Virus en la actividad de sistemas	4	1	4	1	4	2	8	1	4	1	4
7	Incendios en la actividad de Internet	2	3	6	3	6	4	8	3	6	4	8
8	Incendios en la actividad de Sistemas	2	3	6	3	6	4	8	3	6	4	8
9	Sismos durante la actividad de Internet	4	2	8	2	8	1	4	4	16	2	8
10	Sismos durante la actividad de Sistemas	4	2	8	2	8	1	4	4	16	2	8
11	Atentados en la actividad de Internet	1	4	4	4	4	4	4	4	4	4	4
12	Atentados en la actividad de Sistemas	1	4	4	4	4	4	4	4	4	4	4
13	Ataque de hackers	4	1	4	1	4	2	8	1	4	1	4

Riesgo (R) = Probabilidad Ocurrencia (P) x Gravedad (G)

1.4 Conclusiones

El análisis de riesgo realizado para EMAPE S.A. constituye un análisis inicial de los riesgos asociados al desarrollo de las actividades informáticas al interior de la Institución. Este análisis en particular permite establecer un estado inicial de referencia sobre el cual compara los riesgos en los escenarios identificados y que potencialmente pueden desarrollarse durante el quehacer cotidiano.

Los resultados del análisis indican que los escenarios que presentan mayor riesgo del tipo exógeno son: corte de fluido eléctrico, problemas con el circuito digital. Servidor DNS, problemas naturales y de infraestructura; y los escenarios que presentan mayor riesgo del tipo endógeno son; inoperatividad de equipos de comunicación e infraestructura

Dado que más de una actividad (relacionada al Plan de Contingencia) de la Gerencia de Administración y Finanzas guarda estrecha relación con las funciones de otra dependencia como la Gerencia de Infraestructura se hace necesario un nivel de estrecha coordinación entre áreas.

2 PLAN DE CONTINGENCIAS

Introducción

La Gerencia de Administración y Finanzas de EMAPE. cuenta con un Plan de Evacuación, el cual permite a los Brigadistas operativos conocer anticipadamente las acciones a ejecutar cuando las circunstancias lo requieran. a fin de contribuir a minimizar o neutralizar efectos del desastre.

Por su parte la Sub Gerencia de Tecnologia de Información, responsable del monitoreo del parque informático. cuenta con un proceso de copias de seguridad (Backup). dicha información se almacena en los servidores de Backup y es copiado todos los viernes a un disco duro externo

La información de trabajo del personal de la institución se guarda como copia de respaldo. es toda aquella información que es depositada o trabajada en los repositorios compartidos por cada Gerencia. así como la Base de Datos de los Sistemas de EMAPE y los aplicativos son respaldados por la Oficina de Soporte Tecnológico.

La información del usuario que está almacenada en el disco duro de la computadora respectiva de trabajo, cuenta de correo. o cualquier otro dispositivo de almacenamiento o unidad de trabajo diferente al indicado en el párrafo anterior. es total responsabilidad de cada trabajador. Jefe y/o Gerencia. es decir. no es responsabilidad de la Gerencia de Administración y Finanzas.

2.1 Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento, mantenimiento preventivo y correctivo del parque informático y ejecución de las activicades de resguardo de la información e identificación de las prioridades de restauración de los Sistemas Informáticos que nos aseguren un tiempo de respuesta aceptable y óptima, y que implique el menor costo posible a nuestra institución.

Se han establecido los procedimientos relativos al Mantenimiento de equipos, impresoras y Servidores, Copia de Respaldo (backups) e Instalación/Actualización de Software de Antivirus

Para poder efectuar en forma óptima y en el menor tiempo posible las actividades descritas anteriormente se debe conocer lo siguiente:

- Reconocer el ambiente donde se encuentran los Servidores criticos de EMAPE S.A. y el saber identificar a cada uno de ellos Para ello en el **Anexo 1** adjunto al presente Plan se detalla la **"Sala de Servidores"**, donde se muestra la distribución de equipos informáticos, y los equipos de comunicación.

- Conocer los procedimientos a realizar para ofrecer los servicios criticos de EMAPE S.A. a través de la Oficina de Soporte Tecnológico

- Gestionar adecuadamente los Activos de Software para contar con un Inventario de Software por cada computadora de los usuarios, que facilite una rápida identificación y restauración del software instalado.

A continuación se detallan los mantenimientos preventivos por equipo informático realizados en EMAPE S.A.

Mantenimiento Preventivo por Equipo Informático

Equipo	Acción Preventiva / Correctiva	Responsable
Computadoras Personales	Revisión, limpieza interna y externa de todos los componentes. Revisión de virus.	Gerencia de Administración y Finanzas. Terceros (si equipo tiene garantía)
Impresoras	Limpieza interna	Gerencia de Administración y Finanzas. Terceros (si equipo tiene garantía)
Servidores	Se realiza un monitoreo a través de acciones manuales en la consola del servidor. Limpieza interna.	Gerencia de Administración y Finanzas.

a. **Sistemas de Información**

Se detallan la relación de los niveles de prioridad con su puntaje que se aplicarán a los Sistemas desarrollados por la Sub Gerencia de Tecnología de Información o por terceros.

Niveles de Prioridad de Sistemas de Información	
Prioridad	**Puntaje**
Baja	1
Media	2
Alta	3

A continuación se muestra la lista de Sistemas de Información ordenados por prioridad de restauración (desde la máxima prioridad hasta la más baja), que son necesarios para garantizar una continuidad de la operatividad y servicios que ofrece EMAPE S.A ante un desastre o siniestro:

SISTEMAS DE INFORMACIÓN / SERVICIOS IMPLEMENTADOS

SISTEMA DE INFORMACIÓN	PROVEEDOR	PLATAFORMA	LENGUAJE DE PROGRAMACIÓN	USUARIOS	PRIORIDAD
PORTAL	DESARROLLO PROPIO	MySQL, BAJO LINUX (APACHE)	PHP	TODAS LAS GERENCIAS, PÚBLICO EN GENERAL	3
INTRANET	DESARROLLO PROPIO	MySQL, BAJO LINUX (APACHE)	PHP, JAVASCRIPT	TODAS LAS GERENCIAS	3
CORREO	LINUX SUSE	MySQL BAJO LINUX	PHP, AJAX	TODAS LAS GERENCIAS	3
GEMA (VARIOS)	DESARROLLO PROPIO	SQL, BAJO WINDOWS	VISUAL BASIC	TODAS LAS GERENCIAS	3

(Trámite Documentario, Activo Fijo y Contratos)					
GEM WEB (VARIOS)	DESARROLLO PROPIO	SQL, BAJO LINUX (TOMCAT, APACHE)	PHP, ASP.NET	TODAS LAS GERENCIAS	3
OPERACIONES (Mantenimiento de afiliados, Clientes PostPago, Control de Exonerados, Sire Web, Registro de Ocurrencias); RECURSOS HUMANOS (Bienestar, Planillas, Asistencia Planillas, Asistencia SNP, Planilla Obreros); GENERAL (Gestión de la Calidad, Registro de Quejas y Sugerencias, Registro de actividades oficiales, Requerimientos de Bienes y Servicios, Solicitud de Honorarios, Generación de TXT COA Estado, Solicitud de Vehículos)					
VISUAL ASSIST (REGISTRO BIOMETRICO)	PROVEEDOR EXTERNO (DMS)	SQL, BAJO WINDOWS	VISUAL BASIC	RRHH	3
INFORMACIÓN JURÍDICA (SPIJ)	MINISTERIOD E JUSTICIA	WINDOWS	FOLIOS VIEW	Gerencia de Asuntos Legales	1

b. Equipos de Cómputo

La Gerencia de Administración y Finanzas mantiene un inventario de los equipos de informática, estos equipos conforman el parque informático de EMAPE, a continuación se mostrará la tabla de distribución del parque informático:

DISTRIBUCIÓN DE EQUIPOS INFORMÁTICOS

N°	GERENCIAS	N° DE COMPUTADORAS	N° DE IMPRESORAS	N° DE LAPTOPS	N° DE PROYECTOR	N° DE PLOTER	N° DE SCANER
1	DIRECTORIO	1	1	2	1	0	0
2	GERENCIA GENERAL	12	5	2	0	0	2
3	GAF	87	22	6	1	0	1
4	GPP	13	3	2	1	0	0
5	GI	56	8	1	0	1	0
6	GEP	37	3	1	0	1	0
7	GO	13	3	0	0	0	0
8	GAL	10	1	1	0	0	0
9	OCI	7	2	0	0	0	0
TOTAL		236	48	15	3	2	3

c. Obtención y Almacenamiento de los Respaldos de Información

La Gerencia de Administración y Finanzas realiza copias de respaldo a la siguiente información

Software:

- De Base de Datos
- De Aplicativos/Programas
- De archivos de trabajo ubicados en los repositorios compartidos de las Gerencias

Hardware:

No se cuenta en la actualidad con respaldo de equipos Servidores ubicados en el local Institucional, siendo éstos los siguientes: Base de Datos, Portal, Correo, Intranet, Firewall y DNS y demás servicios. Sin embargo a fin de cumplir con lo dispuesto en la NTP-ISO/IEC 17799:2004 EDI que en el acápite 11.1.4 inciso c) del *"Marco de planificación para la continuidad del negocio" menciona: "los procedimientos de emergencia que describan las acciones a realizar para desplazar de forma temporal a lugares alternativos las actividades esenciales del negocio o soportar servicios para devolver la operatividad a los procesos del negocio en el plazo requerido"*, se recomienda que se debe contar en el más breve plazo con Rediseño total de la infraestructura de la sala de servidores o la posibilidad de un Centro de Datos Alternativo bajo la modalidad de Alojamiento (Hosting o Housing) en una empresa de reconocimiento comprobado en el medio.

d. **Políticas (Normas y Procedimientos de backups)**

La Gerencia de Administración y Finanzas, responsable del monitoreo informático, tiene establecido procedimientos, para obtener copias de seguridad de Base de Datos, Aplicativos y Archivos de trabajo de los repositorios compartidos de las Gerencias.

e. **Entrenamiento**

En el plan de trabajo institucional debería considerar tener programado ejecutar diversas actividades de capacitación teórica y práctica contra diferentes tipos de siniestros que afecten el parque informático y la información Institucional, en ese sentido la alta dirección, debería considerar programar eventos para orientar y concientizar a los trabajadores de la Institución respecto a su papel protagónico ante estas amenazas.

2.2 Actividades durante el desastre

2.2.1 Plan de Emergencia

La Gerencia de Administración y Finanzas, pondrá en ejecución el Plan de Evacuación cuando se produzcan desastres de diversos tipos, y en esto, los brigadistas juegan un rol importante, por su parte el personal de Informática actuará paralelamente en los rubros inherentes a su actividad.

Al respecto, la Sub Gerencia de Tecnología de Información proporciona una relación de su personal, la misma que será utilizada en caso de producirse algún incidente informático. Esta lista debe alcanzarse al personal de seguridad y vigilancia de EMAPE S.A. para los casos de horario de fines de semana y/o feriados si se diera la necesidad.

Procedimiento en caso de emergencia

El siguiente procedimiento de acción, especifica los pasos que se deberán seguir en casos de emergencia. Este procedimiento podrá ser modificado para incorporar información adicional que sea pertinente

a Determinar la ubicación del incidente, estimar el tamaño y el tipo de incidente.

b. Llevar a cabo acciones especificas para controlar la armonía informática.
c Notificar la ocurrencia a los responsables de la Oficina de Soporte Tecnológico.
d. Modificar las operaciones para evitar la re-currencia potencial del incidente
e. Documentar el incidente.

A continuación se muestra un cuadro resumen de procedimientos durante la emergencia:

Procedimiento durante la Emergencia		
Horario	**Ocurrencia**	**Acción a Seguir**
Laboral	Problemas en el funcionamiento de computador personal.	Avisar a la SGTI vía correo, teléfono, informe, personalmente.
Laboral	Problemas en el portal, correo, internet y comunicaciones.	Avisar a la SGTI vía correo, teléfono, personalmente.
No Laboral	Problemas en portal, correo, internet y comunicaciones.	Avisar al agente de seguridad encargado del piso o puerta, quien notificará al personal de la lista de números telefónicos de emergencia.
Laboral	Siniestro	Avisar a la SGTI vía correo, teléfono, informe, personalmente
No Laboral	Siniestro	Avisar al vigilante más cercano quien notificará al personal de la lista de números telefónicos de emergencia.

Números Telefónico en caso de Incidentes Informáticos				
Contacto	**Cargo**	**Teléfono**		
		Oficina	**Anexo**	**Correo**
José León Ambia	Gerente de Administración y Finanzas	208-0000	301	aleon@emape.gob.pe
Dante Antiporta Pomacaja	Sub Gerente de Tecnología de Información	208-0000	210	dantiporta@emape.gob.pe
Edward Ncle Nolasco	Soporte Técnico / Servicios de Internet / otros	208-0000	212	enole@emape.gob.pe
Alexander Garay Ruiz	Soporte Técnico / Servicios de Internet / otros	208-0000	212	agaray@emape.gob.pe
Alex Salcedo	Soporte Técnico / Servicios de Internet / otros	208-0000	212	asalcedo@emape.gob.pe
Jessica Poma Espinal	Analista Programador	208-0000	211	jpoma@emape.gob.pe
Kristel Silva	Analista Programador	208-0000	211	ksilva@emape.gob.pe

2.2.2 Formación de Equipos

La Gerencia de Administración y Finanzas, a través del comité de Defensa Civil de EMAPE (en caso de existir), deberá contar con Brigadistas que deben ser designados por los Gerentes de cada una de las Gerencias, quienes actuarán inmediatamente en la lucha contra incendios, evacuación y primeros auxilios, asimismo, harán uso de extintores contra incendios y por su parte, personal de la Sub Gerencia de Tecnología de Información, se encargará del aspecto de recursos informáticos de acuerdo a la clasificación de prioridades.

Equipo Mínimo de Respuesta	
Equipos	**Cantidad**
Servidores de Base de Datos y Aplicativos	5
Lectores Multimedia	5
Extintores de polvo químicos	4
Switches	5
Patch Cord	12
Switch Wireless	2
Proyector Multimedia	1
Herramientas y otros	Varios

2.3 Actividades Después del Desastre

2.3.1 Evaluación de Daños

Inmediatamente después que el siniestro haya concluido, los Brigadistas y el personal de la Sub Gerencia de Tecnología de Información realizarán en primer caso, una evaluación de los bienes materiales, equipos y Sistemas de Información que se hayan visto afectados por el siniestro, indicando cuales pueden ser recuperados y en cuanto tiempo.

2.3.2 Priorización de Actividades del plan de Acción

Las Oficinas involucradas en el Plan de Contingencia de acuerdo al ámbito de su competencia, previa evaluación de los siniestros priorizan las actividades correspondientes, a fin de habilitar los ambientes y poner en funcionamiento en el término perentorio los equipos, sistemas operativos y sistemas de aplicación de la institución. En materia de informática se dará prioridad a las actividades estratégicas y urgentes las cuales pueden ser:

- Habilitación de servidores si fuera el caso que estén dañados.
- Restauración del último Backup de datos de los sistemas en producción.
- Reinstalación de los Sistemas de Información de acuerdo al Cuadro de Prioridades en las PCS clientes.
- Reinstalación de Sistemas Operativos y Software Base en los terminales que se encuentren operativos en ese momento, si es que presentasen problemas.
- Puesta en marcha del Centro de Datos de Respaldo Alternativo (Data Center Backup).

Acciones Correctivas a tomar Después del Desastre			
Equipo Informático Afectado	**Acción Correctiva**	**Tiempo Estimado**	**Dependencia / Área Responsable**

Equipos de Red: Hub, Switch	Se reemplaza con Switch, Hub o Router Inalámbrico del Stock de equipos informáticos (Si hubiera).	60 minutos	GAF - SGTI
Impresoras matriciales, inyección de tinta o láser	Se reemplaza por una impresora del mismo tipo si hay disponibilidad en stock de equipos informáticos. Caso contrario se utilizará impresora de red de la misma área o de otra área.	20 minutos	GAF - SGTI
Equipos Comunicación Routers	No se cuenta con stock de este equipo	7 - 8 horas	GAF - SGTI
Computadores Personales	Se reemplaza con equipo disponible en el stock de equipos informáticos. Si el equipo tiene garantía y presenta fallas se acude al CAS del fabricante.	40 minutos No determinado	GAF - SGTI CAS al llamado de GAF - SGTI
Servidor Portal, Servidor Intranet, Servidor Base de Datos, Servidor Correo.	Puesta en marcha del Centro de Datos de Respaldo Alternativo (en el caso de que esta solución ya esté operativa).	8 horas	GAF - SGTI - Empresa Proveedora de la salida a internet
Servidor Portal, Servidor Intranet, Servidor Base de Datos, Servidor Correo. Servidor Fileserver Servidor DNS / Firewall	Se reemplaza con Servidor Backup de Portal, Servidor Backup de Intranet, Servidor Backup de Base de Datos o Servidor Backup de Correo ubicados en el local Institucional. Se realizan acciones de reinstalación y configuración. Se reinstala y reconfigura el Servidor DNS ubicado en la sala de los Servidores	8 horas No determinado 8 horas	GAF - SGTI Representante al llamado de la GAF - SGTI. GAF - SGTI

2.3.3 Ejecución de actividades

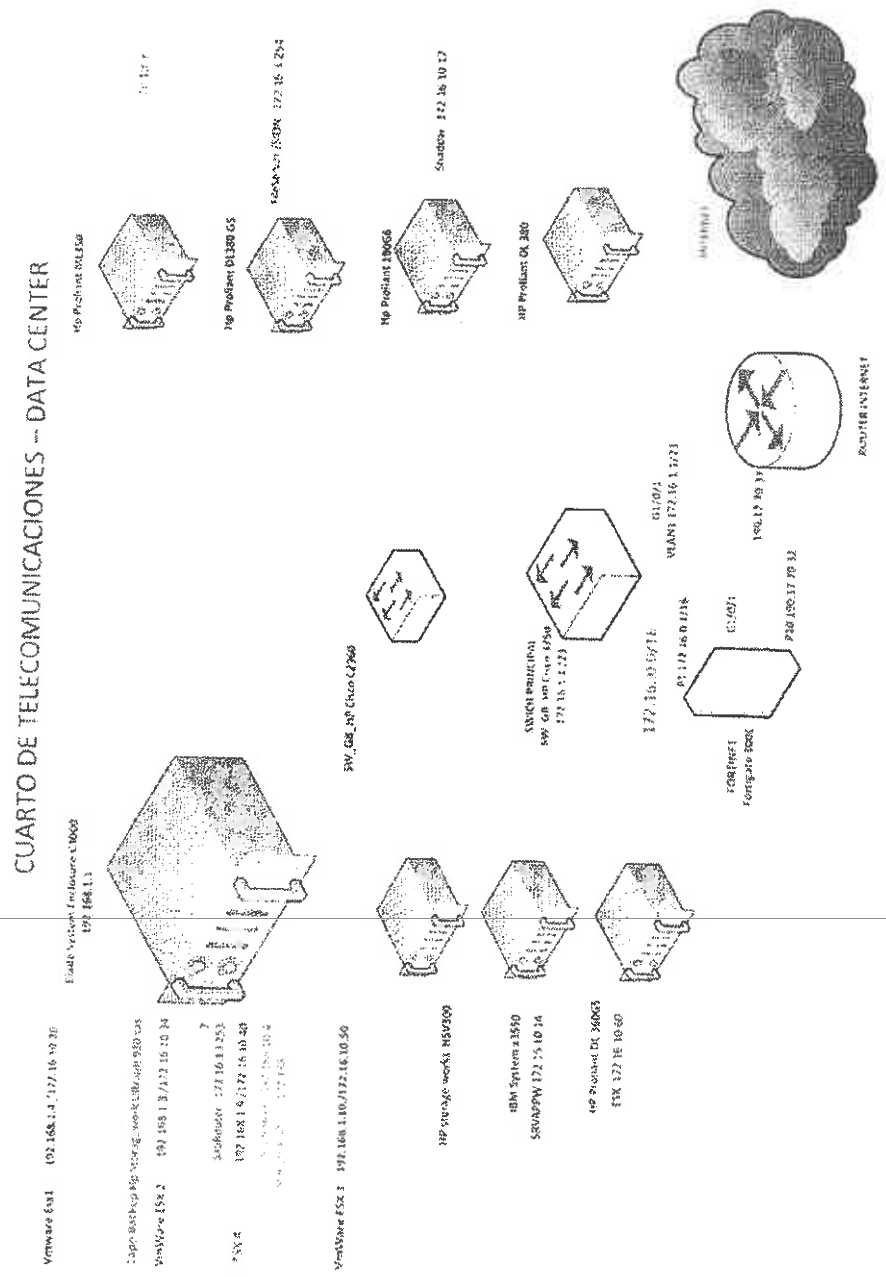
Los brigadistas, en forma coordinada con los responsables de la Sub Gerencia de Tecnología de Información de la Sede Central de EMAPE S.A., actuarán en forma conjunta para la ejecución de las específicas para casos de emergencia.

2.3.4 Retroalimentación del Plan de Acción

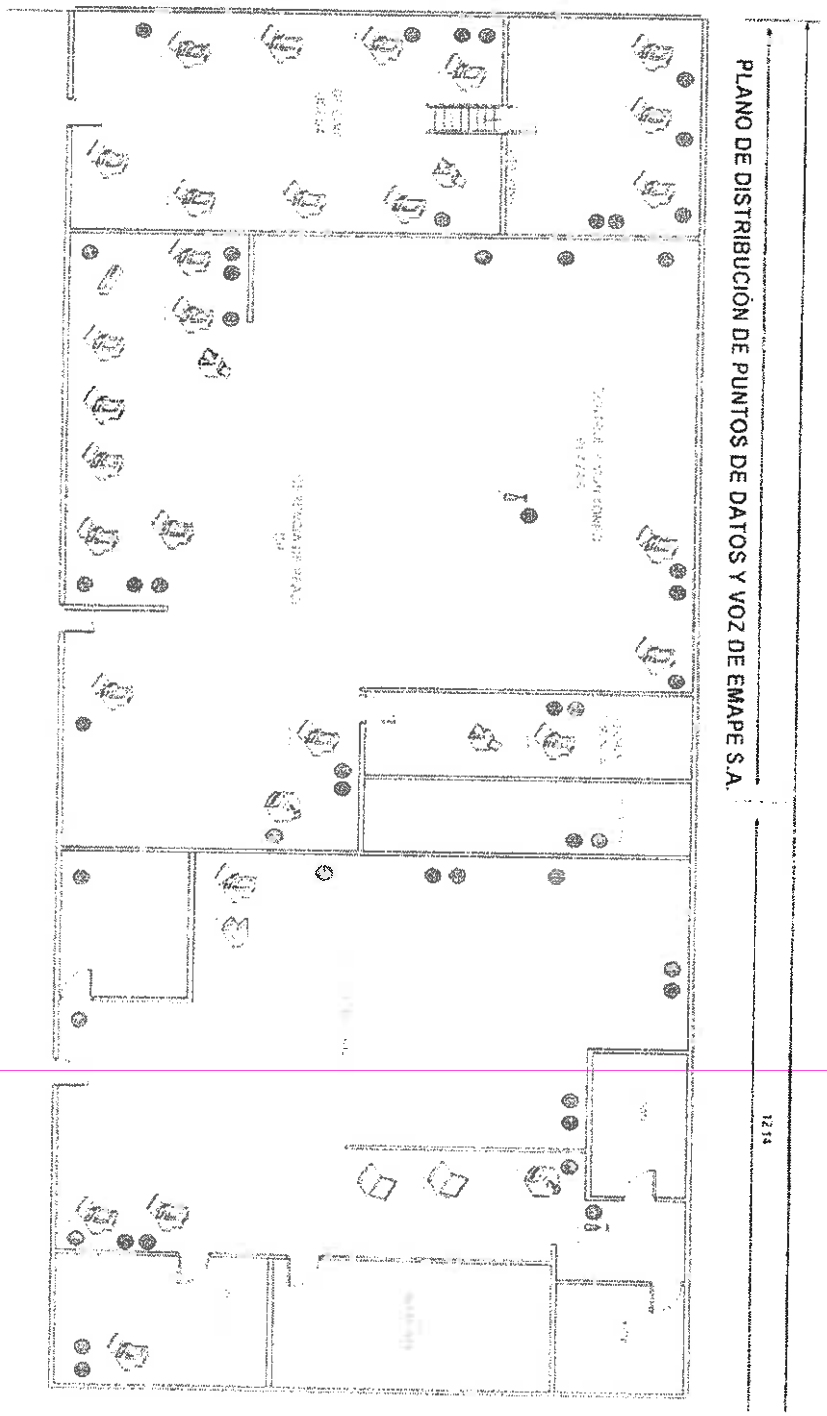
El Plan de Contingencia es un documento de gestión de la Gerencia de Administración y Finanzas, teniendo la característica de tener contenidos que cambian en el tiempo, vale decir que van acorde con las emergencias que se podrían suscitar y con los cambios tecnológicos de los equipos informáticos; cuya información tendrá que incorporarse al documento en el marco de una retroalimentación constante, garantizando la vigencia y utilidad de este Plan.

ANEXOS

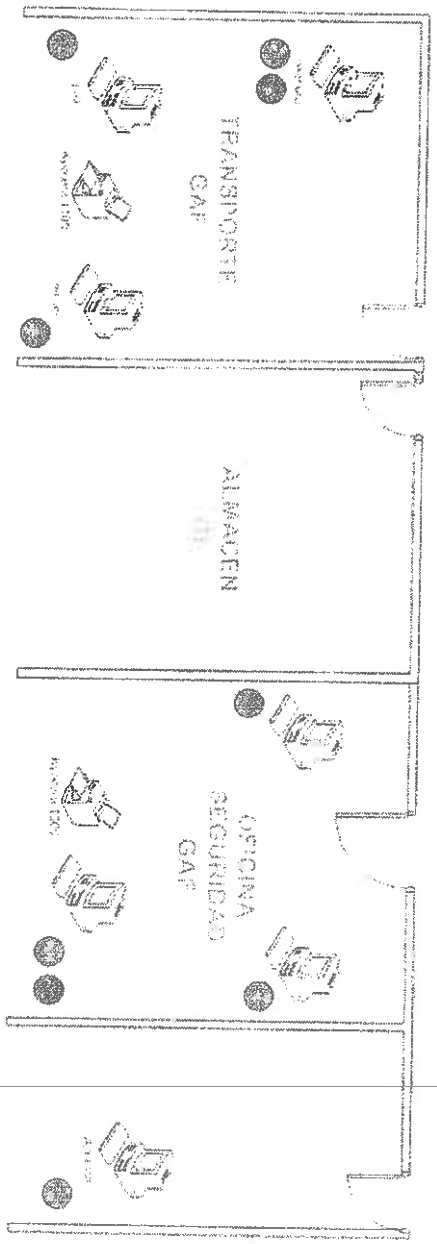
ANEXO 01

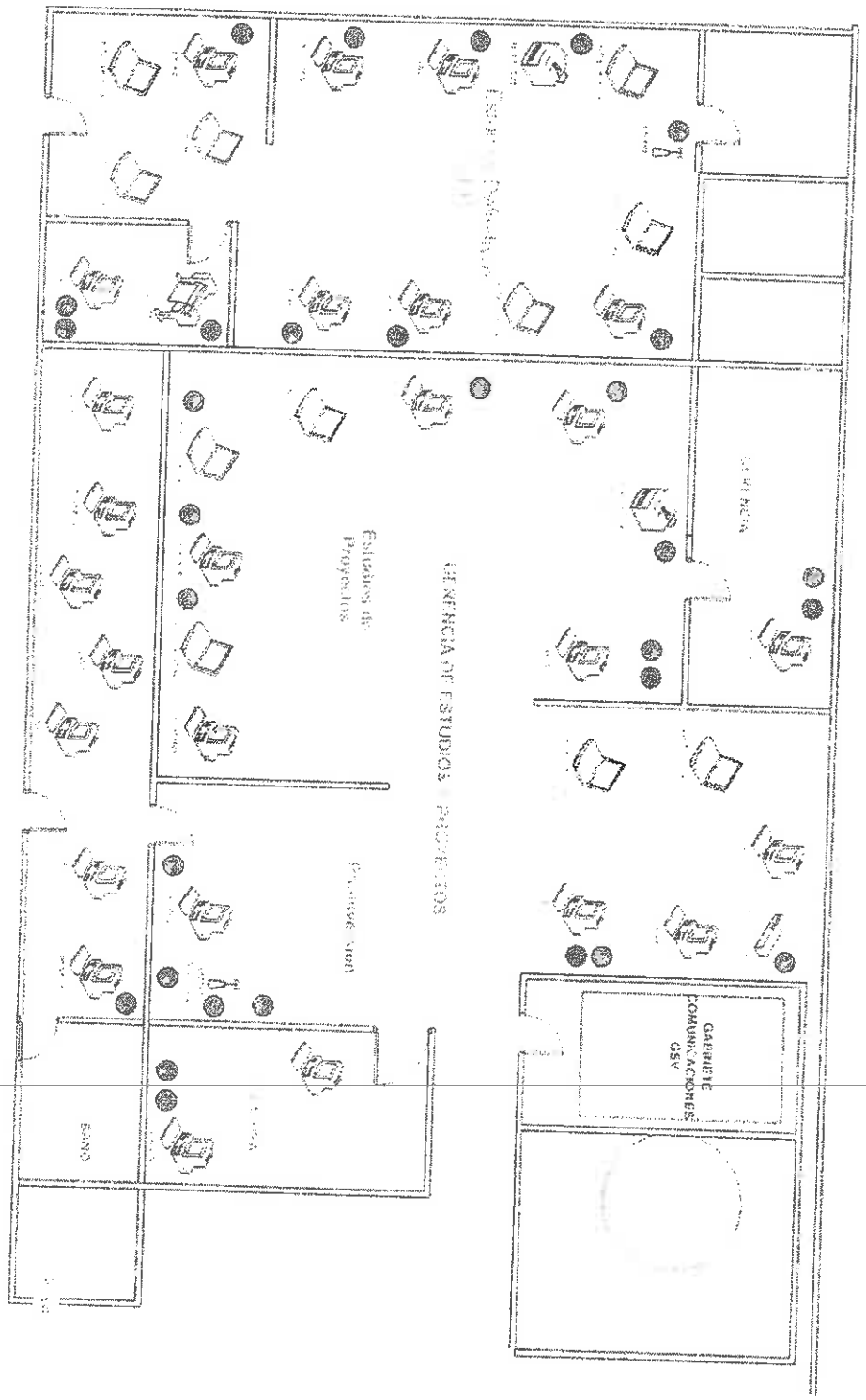


ANEXO 02



PLANO DE DISTRIBUCIÓN DE PUNTOS DE DATOS Y VOZ DE EMAPE S.A.


TRANSPORTE
GAF
ALMACEN
GAF
SEGURIDAD
GAF


GERENCIA DE ESTUDIOS Y PROYECTOS
Estudios de Proyectos
GABINETE COMUNICACIONES GSV