PLAN DE CONTINGENCIA INFORMÁTICA DEL SISTEMA METROPOLITANO DE LA SOLIDARIDAD – SISOL

2018

Control de Cambios

Fecha	Versión	Descripción	Responsable
02/05/2018	1.0	Elaboración del documento	Marlon Arturo Falla Castro

MUNICIPALIDAD METROPOLITANA DE LIMA
V°B°
MARLON FALLA CASTRO
JEFE USP
Sistema Metropolitano de la Solidaridad

ÍNDICE

1. Introducción

El Plan de Contingencia Informático del SISOL (en adelante, EL PLAN), es un documento que establece estrategias de respuestas para restablecer las operaciones y servicios informáticos del SISIOL en forma oportuna, eficiente y eficaz, ante un desastre o evento que afecte la plataforma tecnológica, sistemas de información y sus procedimientos.

Durante el desarrollo de EL PLAN, se presentarán actividades de gestión de riesgos, las vulnerabilidades y amenazas a las cuales el SISOL está expuesto, así como también, las contingencias, acciones preventivas y planes de acción a tomar en cuenta para amenguar el impacto o reducir la probabilidad de ocurrencia de eventos adversos. En ese sentido, EL PLAN brindará un panorama detallado de las contingencias, las mismas que podrán servir como marco de referencia para la elaboración de las políticas, normas y procedimientos complementarios.

2. Base Legal

1. DL. Nº 604, Ley de Organización y Funciones del INEI.
2. DS. Nº 018-91-PMC, Reglamento de Organización y Funciones del INEI.
3. RJ. Nº 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
4. RJ. Nº 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
5. RJ. Nº 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
6. Ley orgánica de Municipalidades Nº 27972 Artículo 20° inciso 6) del 27-05-2003 (Dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas).
7. Ordenanza Nº 683 de la Municipalidad Metropolitana de Lima crea el "SISTEMA METROPOLITANO DE LA SOLIDARIDAD".

MUNICIPALIDAD METROPOLITANA DE LIMA V°B° MARLON FALLA CASTRO JEFE/USP Sistema Metropolitano de la Solidaridad

3. Objetivo

3.1. Objetivo General

Formular EL PLAN acorde a la realidad del SISOL, el cual permita brindar continuidad en los servicios informáticos críticos del SISOL, así como establecer acciones y procedimientos preventivos ante los riesgos a los cuales se encuentra expuesto la institución.

3.2. Objetivos Especificos

✓ Contar con documentación práctica y actualizada que brinde al SISOL procedimientos de contingencia y recuperación de las operaciones informáticas sin sufrir paralizaciones o pérdidas relevantes.

- ✓Identificar y analizar los posibles riesgos que pueden afectar las operaciones informáticas de la institución.

- ✓Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupciones relevantes.

- ✓Preparar al personal para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del SISOL.

4. Alcance

El PLAN ha sido elaborado de acuerdo con las necesidades y realidad actual del SISOL y es aplicable a la recuperación de los sistemas informáticos, procesos, bases de datos, equipos de comunicaciones e infraestructura informática en las oficinas administrativas y los establecimientos de salud a nivel nacional.

5. Generalidades

5.1. Definición de Incidente

En el campo de las tecnologías de la información un incidente se define como cualquier evento que no forma parte del desarrollo habitual de un servicio, el cual puede causar una interrupción del mismo o una reducción en la calidad.

5.2. Definición de Contingencia

En términos generales la contingencia suele referirse a algo que es probable que ocurra, aunque no se tenga una certeza al respecto. La contingencia, por lo tanto, es lo posible o aquello que puede, o no, concretarse.

V°B° MARLON FALLA CASTRO JEFE USP Sistema Metropolitano de la Solidaridad

En el campo de las tecnologías de la información en la empresa la contingencia se define como la alteración en la continuidad del negocio, que impacta en forma relevante el normal desarrollo de un servicio considerado crítico, teniendo su origen en la falla de uno o varios componentes o la interrupción de una tarea.

5.3. Definición de un Plan de Contingencia Informática

El PLAN es una herramienta de gestión necesaria para dar una respuesta planificada ante las contingencias que puedan ocurrir en el dominio de las tecnologías de la información y comunicaciones e interrumpan los servicios informáticos. Así mismo, debe contener las medidas, las técnicas, la organización, los roles, las funciones y los procedimientos necesarios para la recuperación de las operaciones de la compañía luego de ocurrida la contingencia.

Un plan de contingencias es un caso particular del plan de continuidad de negocio aplicado por la Gerencia de Tecnología de la Información. Otros

departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista.

5.4. Gestión de la Continuidad del Negocio

El objetivo de la gestión de la continuidad del negocio en el campo informático se enfoca en la continuidad de los servicios que son soportados por las tecnologías de la información, controlando los riesgos que podrían impactar seriamente dichos servicios.

La gestión de la continuidad del servicio TI (IT Service Continuity Management, ITSCM) es parte del diseño del servicio (ITIL Fundation v3), el cual se ocupa de que el proveedor de servicios de TI siempre pueda proveer un mínimo nivel del servicio propuesto reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación de los mismo.

6. Metodología

Para elaborar EL PLAN se seguirá una metodología que tiene las siguientes fases:

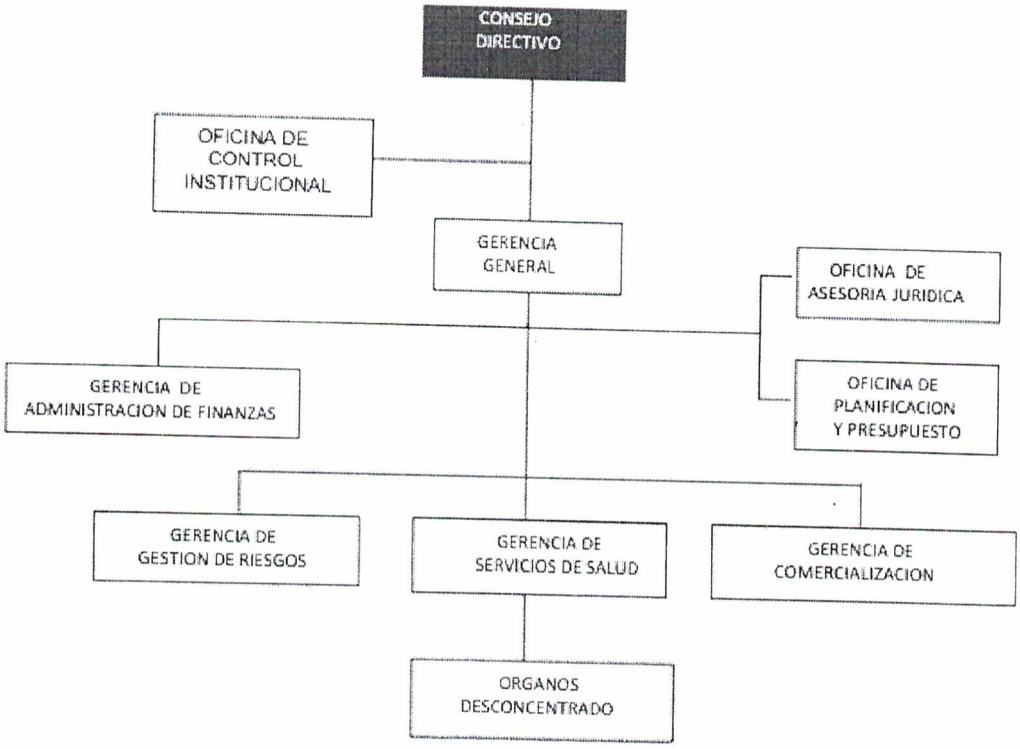
- ✓ Fase 1: Organización
- ✓ Fase 2: Situacional Actual de las Tecnologías de la Información
- ✓ Fase 3: Identificación y Análisis de Riesgos
- ✓ Fase 4: Procedimientos de Contingencia Informática
- ✓ Fase 5: Desarrollo de los Planes de Acción
- ✓ Fase 6: Definición y ejecución del plan de pruebas
- ✓ Fase 7: Disposiciones Finales

MUNICIPALIDAD METROPOLITANA DE LIMA V°B° MARLON FALLA CASTRO JEFE USP Sistema Metropolitano de la Solidaridad

7. Organización

7.1. Estructura organizacional

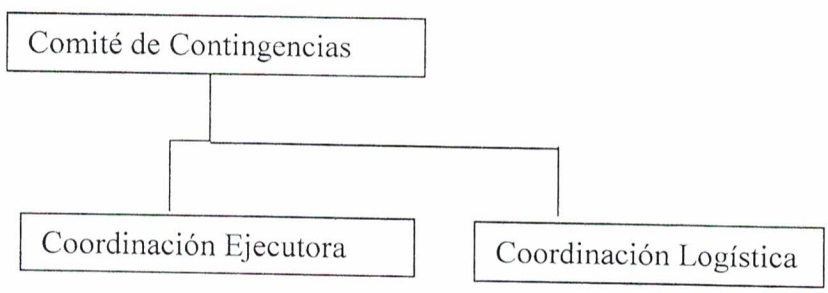
La estructura organizacional nos muestra el esquema funcional de la institución, permitiendo identificar a actores y roles que se desempeñarán en EL PLAN. A continuación se presenta el organigrama del SISOL:



7.2. Organización Ante Contingencias

El plan de contingencia deberá plantearse de manera que la organización pueda prevenir fallas o accidentes en sus operaciones diarias permitiendo seguir activas en la provisión de servicios.

En ese sentido, EL PLAN debe de formularse de manera formal y responsable, de tal forma que involucre en mayor o menor medida a toda la organización en los procesos de prevención, ejecución y recuperación, pero definiendo un grupo especializado para su elaboración, validación y mantenimiento, por lo que se propone la siguiente organización ante contingencias informáticas en el SISOL.



7.3. Comité de Contingencias

El Comité de Contingencias es el órgano donde se coordinará, planeará y aprobarán todas las actividades planteadas, lineamientos, políticas y mejoras

a EL PLAN que se ejecutarán en caso se activen las contingencias informáticas. Este comité se reunirá por lo menos con una periodicidad anual para tratar mejoras a los procedimientos y lineamientos.

✓ *Miembros del Comité del Plan de Contingencias*

- Gerente General
- Gerente de Administración y Finanzas
- Jefe de la Unidad de Sistemas y Procesos
- Otras Gerencias que se consideren pertinentes

✓ *Funciones del Comité del Plan de Contingencias*

- Tomar decisiones en base a EL PLAN ante un incidente o evento que lo active.
- Participar en las reuniones periódicas convocadas por el Coordinador Ejecutor.
- Proponer mejoras a EL PLAN.
- Aprobar los cambios a EL PLAN elaborado por el Coordinador Ejecutor y su equipo técnico.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados con el Coordinador Ejecutor.
- Informar a la Dirección Ejecutiva sobre el impacto económico y de operación de los eventos que hayan activado EL PLAN.

V°B° MIRLON FALLA CASTRO JEFE USP Sistema Metropolitano de la Solidaridad

✓ *Roles del Comité del Plan de Contingencias*

- Miembro del Comité: Integrante permanente del comité, encargado de evaluar y plantear medidas ante la ocurrencia de una contingencia conjuntamente con el Coordinador Ejecutor.
- Presidente del Comité: Encargado de dirigir el comité e invitar a participar a otros participantes.
- Coordinador Ejecutor: Estará a cargo del Jefe de la Unidad de Sistemas y Procesos y se encargará de ejecutar EL PLAN, dirigiendo las acciones de contingencia, proponiendo mejoras e implementando medidas preventivas y correctivas.
- Miembro invitado: Director o Jefe de área del SISOL, la cual ha sido invitado a participar.

7.4. Coordinación Ejecutora

La Coordinación Ejecutora de EL PLAN será la encargada de ejecutar y mantener actualizado EL PLAN en coordinación con el Comité de Contingencias, así mismo, supervisará y coordinará con otras áreas las acciones a llevarse a cabo durante un evento de contingencia.

✓ *Funciones de la Coordinación Ejecutora del Plan:*

- Responsable de la coordinación en la ejecución de EL PLAN.
- Dirigir al equipo de especialista informáticos en la ejecución de las actividades preventivas y correctivas establecidas en EL PLAN a fin de prevenir o restablecer los servicios.
- Evaluar el impacto de las contingencias que se presenten y los riesgos potenciales.
- Activar los procedimientos de contingencia en coordinación con el Comité de Contingencia.
- Informar al Comité de Contingencia de las acciones realizadas ante un evento ocurrido que tenga impacto en las operaciones de la institución.
- Mantener permanentemente actualizado EL PLAN y proponer mejoras en caso se requiera.
- Ejecuta acciones preventivas de acuerdo a lo establecido en EL PLAN.

- Implementar las mejoras a EL PLAN.
- Coordinar que los recursos informáticos de contingencia estén disponibles ante la ocurrencia de eventos adversos y que el personal esté debidamente capacitado para afrontar las contingencias.
- Realizar pruebas de recuperación para la mejora de los procedimientos de contingencia.

✓ *Roles de la Coordinación Ejecutora del Plan:*

- Coordinador Ejecutor: Responsable de activar el Plan y su correcta ejecución, informando en todo momento al Comité Ejecutivo. Además, deberá de implementar medidas preventivas que disminuyan los riesgos o disminuyan el impacto en las operaciones y los tiempos de recuperación de los servicios, así como mantener actualizado el Plan de acuerdo a los cambios en los sistemas e infraestructura tecnológica del SISOL.

- Miembro de Equipo Técnico: Los miembros de equipo técnico se encargarán de la implementación de las acciones, de acuerdo al EL PLAN, que lleven a la recuperación de los servicios informáticos que se afecten al ocurrir una contingencia. Los miembros del equipo técnico deberán cumplir con los siguientes roles:

  - *Analista de Sistemas:* Especialista en los sistemas de información críticos.

  - *Administrador de Base de Datos:* Especialista en la administración de los motores de base de datos que dan soporte a los sistemas de información.

  - *Coordinador de Redes y Comunicaciones:* Especialista en administración de las redes de datos y equipos de comunicaciones.

  - *Soporte Técnico/Encargado de Cómputo:* Especialista en computación que brinda asistencia técnica a nivel usuario en aplicaciones ofimáticas y equipos de cómputo.

  - *Especialista en Seguridad de la Información:* Especialista en establecer controles de seguridad y acceso a la información.

7.5. Coordinación Logística

La coordinación logística estará conformada por un representante de la Gerencia de Administración y Finanzas (Designado por el Gerente de Administración y Finanzas), el cual será responsable de las siguientes actividades de presentarse una contingencia.

MUNICIPALIDAD METROPOLITANA DE LIMA V°B° MARLON FALLA CASTRO JEFE OGP Sistema Metropolitano de la Solidaridad

- ✓ ***Funciones de la Coordinación Ejecutora del Plan:***

  - Responsable de dar las facilidades logísticas para la recuperación de los servicios informáticos en el lugar donde se requiera si la emergencia lo amerita (Habilitación de ambientes, restablecimiento de energía eléctrica, contratación de servicios, insumos, mueblería, transporte, etc.).

  - Coordinar las necesidades logísticas y financieras con el Coordinador Ejecutor para la recuperación de los servicios informáticos.

  - Informar al Comité de Contingencias la ejecución de los presupuestos asignados para la recuperación de las contingencias.

7.6. Sedes del SISOL

Las sedes donde se ejecutarán las actividades del presente Plan abarcan sedes administrativas y los establecimientos de salud de la solidaridad en caso de presentarse una contingencia.

Sedes Administrativas del SISOL		
N°	Sede	Dirección
1	Sede principal	Calle Carlos Concha 162, San Isidro
2	Cabo Blanco	Calle Cabo Blanco 352, San Isidro
3	Ejercito	Av. del Ejercito 2380, Magdalena del Mar

Establecimientos de salud de la Solidaridad - SISOL				
N°	Nombre Establecimiento	Tipo	Ubicación	Dirección
1	Ate-Vitarte	Policlínico	Lima	Av. Rivadeneira Mz. F Lote 5 y 6 Urb. Ceres Telf. 352-0798
2	Carabayllo	Policlínico	Lima	Av. San Martín cdra. 2 s/n - Urb. Santa Isabel Telf. 543-3444
3	Camaná	Policlínico	Lima	Jr. Camaná 700 Telf. 426-4619
4	Chorrillos	Policlínico	Lima	Av. Prolongación Paseo de la República con Av. Fernando Terán 990 Telf. 467-1684
5	Comas	Policlínico	Lima	Av. Túpac Amaru, Km. 7.5, Parque La Merced Telf. 525-5462
6	El Agustino	Policlínico	Lima	Cruce Av. César Vallejo con JC. Mariátegui Telf. 385-0954
7	La Victoria	Policlínico	Lima	Av. Manco Cápac 218 - La Victoria Telf. 272-9421
8	Lince	Policlínico	Lima	Av. Canevaro 550 Telf. 472-6755
9	Magdalena	Policlínico	Lima	Calle Bolognesi 260 Telf. 263-6103
10	Mirones	Policlínico	Lima	Av. Colonial, cdra. 19 Telf. 336-8228
11	Puente Piedra	Policlínico	Lima	Km. 30 de la Panamericana Norte Telf. 548-0573
12	Punta Hermosa	Policlínico	Lima	Antigua Panamericana Sur, Km 43
13	Metro - UNI	Policlínico	Lima	Av. Gerardo Unger, Alt. Cdr. 16 (dentro Metro UNI) Telf. 534-8556
14	San Juan de Lurigancho	Policlínico	Lima	Av. Proceres de la Independencia s/n (Costado de Metro)| Telf. 253-1186
15	San Martín de Porres	Policlínico	Lima	Av. Perú 3811 Telf. 572-1123
16	Surquillo	Policlínico	Lima	Av. Angamos 714 Telf. 243-1120
17	Villa El Salvador	Policlínico	Lima	Av. Pastor Sevilla y Óvalo Pumacahua Telf. 292-3504
18	Villa Maria del Triunfo	Policlínico	Lima	Av. Salvador Allende cdra. 16 Telf. 296-0128
19	EE.SS Rímac (Flor de Amancaes)	Policlínico	Lima	Av. Prolong. Amancaes 1377 (Lima - Lima - Rimac)
20	EE.SS Emmsa	Policlínico	Lima	Av. de la Cultura 808 (Lima - Lima - Santa Anita)
21	EE.SS San Borja (Especialidades Médicas Quirúrgicas)	Policlínico	Lima	Av. San Borja Sur 285 (Lima - Lima - San Borja)
22	Chiclayo	Policlínico	Chiclayo	Paseo de los Héroes, Av. Salaverry Cdras. 6, 7 y 8 Telef. (074) 223232
23	Cusco	Policlínico	Cusco	Urb. Larapa Grande C1-7-B Distrito de San Jerónimo Telef. (084) 276494
24	Ica	Policlínico	Ica	Prolongación Ayabaca s/n (Ovalo de los Maestros) Telef. (056) 221600
25	Sullana - Piura	Policlínico	Piura	Calle Transversal Piura y Calle 2, Barrio Buenos Aires Telef. (073) 639479
26	Tacna	Policlínico	Tacna	Av. Manuel A. Odría s/n Para Chico Telef. (052) 314955
27	Tarapoto	Policlínico	Tarapoto	Jr. Jimenes Pimentel 1309
28	Tumbes	Policlínico	Tumbes	Av. Tumbes s/n (Costado de Coliseo Tumpis) Telef. (072) 790498
29	La Ensenada	Policlínico	Lima Norte	AA.HH. La Ensenada, Valle del Chillón - Puente Piedra Telf. 551-0534

V°B°
MARLON FALLA CASTRO
JEFE USP

30	Las Violetas	Policlínico	Lima Norte	Av. Los Ficus Cdra. 3 s/n - Independencia Telf. 534-5510
31	San Ramón	Policlínico	Lima Norte	Calle Micaela Bastidas, AA.HH. San Ramón - Comas Telf. 542-6404
32	Sinchi Roca	Policlínico	Lima Norte	Jr. Wiracocha Cdra. 2 Urb. San Agustín 2da etapa - Comas Telf. 536-5999
33	El Nazareno	Policlínico	Lima Sur	Jr. Emaus s/n, Pamplona Alta - San Juan de Miraflores Telf. 285-3343
34	Villa Limatambo	Policlínico	Lima Sur	Entre Mz. H/1, San Gabriel Alto - Villa María del Triunfo Telf. 283-4040
35	Centro Materno Infantil Juan Pablo II	Policlínico	Lima Este	Calle 16 s/n, AA.HH. Juan Pablo II - San Juan de Lurigancho Telf. 388-3932
36	Huaycán	Policlínico	Lima Este	Calle 11 s/n, Zona H - Huaycán Telf. 371-6497
37	José Carlos Mariátegui	Policlínico	Lima Este	Av. Continuación s/n AA.HH. San Juan de Lurigancho Telf. 392-2128
38	Señor de los Milagros	Policlínico	Lima Este	Jr. Las Margaritas s/n - San Juan de Lurigancho Telf. 388-4478
39	Trabajadores Hospital del Niño	Policlínico	Lima Este	Av. Polonia s/n - San Juan de Lurigancho Telf. 387-0490
40	Medicina Estilo de Vida	Policlínico	Lima	Calle Las Aguilas 378, Surquillo, Telf. 2775105

8. Situación Actual de las Tecnologías de la Información

El SISOL es un Órgano Público Descentralizado (OPD) de la Municipalidad Metropolitana de Lima, el cual ofrece a la población servicios de salud de calidad brindando bienestar de las familias de Lima Metropolitana y del interior del país.

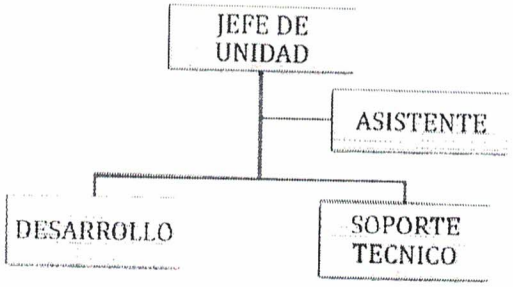
Uno de sus principales objetivos es atender a la población con tecnología moderna calidad, calidez, innovación, rapidez, oportunidad a tarifas accesibles. Para poder lograr el objetivo, el SISOL cuenta con una plataforma tecnológica que da soporte a diversos servicios que ofrece a la población y a sus tareas administrativas y su administración está a cargo de la Unidad de Sistemas y Procesos.

8.1. Unidad de Sistemas y Procesos (USP)

La Unidad de Sistemas y Procesos es la unidad encargada de planear, dirigir y supervisar las tecnologías de la información (TI) de la institución orientadas a la prestación de los servicios de salud.

Entre sus funciones está la de la elaboración y ejecución del Plan de Contingencias Informático que ayude a la institución a recuperar los servicios informáticos con el menor impacto posible al presentarse una interrupción de consideraciones en las operaciones.

A continuación, se presentan la siguiente estructura de acuerdo a las funciones que realiza.



8.2. Recursos Institucionales

El SISOL cuenta con los siguientes recursos para la puesta en marcha del presente plan:

a. Humanos

Están dados por las personas que participan directa o indirectamente en el desarrollo de EL PLAN, siendo la USP quienes ejecutaran los procedimientos de recuperación.

EL PLAN deberá contar con el respaldo y apoyo de la Dirección Ejecutiva y las gerencias del SISOL al comprender la importancia del mismo.

El personal que tenga participación directa en la ejecución EL PLAN será entrenado y participará en las pruebas de contingencia para obtener el máximo provecho de acuerdo a los roles que desempeñan.

b. Materiales

Todas las herramientas de soporte, material de escritorio, equipos de cómputo y comunicaciones e insumos informáticos, necesario para llevar a cabo EL PLAN.

c. Financieros

Los recursos financieros que se requiere contar para la aplicación de EL PLAN serán dispuestos por el Comité de Contingencias.

8.3. Catálogo de Servicios Informáticos

La USP brinda los siguientes servicios informáticos:

- ✓ Servicio de correo electrónico.
- ✓ Servicio de administración de la Web Institucional.

- ✓ Servicio de administración de servicios de aplicaciones de negocio.
- ✓ Servicio de Internet.
- ✓ Servicio de Soporte Técnico.
- ✓ Servicio de seguridad informática.
- ✓ Servicio de soporte especializado en aplicaciones.
- ✓ Servicio de administración de servidores de aplicaciones.
- ✓ Servicio de Desarrollo de software.
- ✓ Servicio de explotación de datos.
- ✓ Servicio de instalación y mantenimiento de equipos de cómputo.
- ✓ Servicios de conectividad de redes de datos.

8.4. Activos Informáticos

Los activos informáticos son todos los componentes de hardware (equipos de cómputo, componentes, impresoras, equipos de comunicaciones, redes de datos), de software y procesos que dan soporte a los servicios informáticos.

Los activos informáticos con los que dispone el SISOL son los siguientes:

a. Equipos de Informáticos

Tipo	Cantidad
Servidores	25
Equipos de Computo	876
Impresoras (Multifuncional, Ticketeras, Inyección, Laser, Matricial)	559

b. Software Utilizado

El software utilizado en el SISOL se muestra en el siguiente cuadro:

Descripción	Administrado por
MS Windows 2003 server (5es)	USP
MS Windows 2003 server cal	USP
MS Windows 2012 server	USP
MS Windows 2012 server cal	USP
CentOS 6.5	USP
CentOS 7	USP
MS Windows 7 Profesional	USP
MS Windows 8 Profesional (laptops)	USP
Microsoft SQL Server 2000 y 2008	USP
Postgress (libre)	USP
Mysql (libre)	USP

MS office 2013 OEM	USP
MS office 2010 Standard	USP
Autocad 2017	Infraestructura
Forticlient	USP
SPIJ (Sistema del Poder Judicial)	Asesoría Jurídica
Software para Costos y Presupuestos S10	Presupuesto
Firma Digital	USP

c. Aplicativos Informáticos

N°	Nombre	Descripción	Tipo	Administrado por	Responsable funcional
1	SIGHO (Crítico)	Sistema de Gestión Hospitalaria	Línea	USP	Gerencia de Salud Gerencia de Administración y Finanzas
2	ZINCRON	Sistema de Control de Asistencia	Soporte	RRHH	RRHH
3	Control Patrimonial	Sistema de Control Patrimonial	Soporte	Patrimonio	Gerencia de Administración y Finanzas
4	PERSON	Registro de Personal del SISOL	Soporte	USP	RRHH
5	Web Service (Crítico)	Servicios de consulta de interconexión con los Establecimientos de salud	Línea	USP	USP
6	Correo electrónico	Servicio de correo electrónico	Línea	USP	USP
7	Página Web	Página Web Institucional	Línea	USP	Comunicaciones USP

V°B°
MARLON FALLA CASTRO
JEFE USP
Sistema Metropolitano de la Solidaridad

d. Servidores

N°	Sistemas Operativos	Funcionalidad	IP
1	Windows Server 2008 R2 Enterprise	Servidor DNS, Active Directory	192.168.101.240
2	CentOS 6.5 (Linux)	Servidor de correo Zimbra 8.0.4	200.62.231.213
3	CentOS 5.10 (Linux)	Servicio de Firewall y Proxy	192.168.101.253
4	CentOS 6.5 (Linux)	Servidor de backup de Base de Datos del SIGHOS	10.10.10.5
5	CentOS 6.5 (Linux)	Servidor de la página Web e intranet	192.168.1.7

Cabe indicar que establecimientos de salud del SISOL disponen de un servidor físico con SIGHOS instalados que soporta la atención del establecimiento. Así mismo backup donde se tiene el aplicativo SIGHOS y en la Sede Central.

e. Redes de datos

La red de datos es mixta, con tendido de cable UTP Cat5 y Cat6, que ha ido creciendo sin un orden establecido tanto en las sedes administrativas como en los establecimientos de salud.

Los equipos de comunicaciones son switches no administrables que no permiten una adecuada segmentación y control de acceso a la red y el uso de la red.

9. Identificación y Análisis de Riesgos

Un riesgo es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas.

Un Plan de Contingencia Informático no solo debe atender la recuperación de las operaciones de TI frente a un desastre, sino también contemplar acciones preventivas. Para esto, se debe efectuar una evaluación de los riesgos que no solo contemple la identificación de amenazas significativas, las vulnerabilidades y el grado de exposición al riesgo, sino que también es necesario identificar los controles a instaurar para minimizar el daño del impacto de un posible desastre en la institución.

9.1. Definición de Eventos Susceptibles de Contingencia

EL PLAN abarca todos los aspectos que forman parte de los activos informáticos, en tal sentido, resulta de vital importancia identificar, detallar y agrupar todos los elementos susceptibles de una contingencia informática:

- ✓ Hardware
  - ➢ Servidores.
  - ➢ Equipos de cómputo (laptops y PC´s).
  - ➢ Impresoras, scanner.
  - ➢ Equipos multimedia.
- ✓ Comunicaciones
  - ➢ Equipos de comunicaciones Switch.
  - ➢ Equipo de comunicaciones Router.
  - ➢ Equipo de Telefonía fija.
  - ➢ Cableado de Red de Datos.
- ✓ Software

- Software de Base de Datos.
- Aplicativos utilizados por el SISOL.
- Software de Aplicaciones.
- Software Base.
- Software Antivirus.

✓ Información

- Base de Datos utilizados por los Aplicativos.
- Respaldo de información generada por los usuarios.
- Respaldo de las Aplicaciones utilizadas por SISOL.
- Respaldos de Base de Datos.
- Respaldos de información y configuración de los Servidores.

✓ Otros equipos

- Grupo Electrógeno.
- UPS.
- Aire Acondicionado.

✓ Infraestructura Física

- Datacenter y gabinetes de comunicaciones en sedes administrativas y establecimientos de salud del SISOL.

✓ Operativos

- Logística operativa (suministros Informáticos).

✓ Servicios Públicos

- Suministro de energía eléctrica.
- Servicio de telefonía fija analógico/digital y móvil.
- Enlace a Internet

✓ Recursos Humanos

- Disponibilidad de personal de la Dirección del SISOL.
- Disponibilidad de personal especialista de la USP.

9.2. Eventos Controlables y No Controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos del SISOL, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

- ✓ Eventos Controlables, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

- ✓ Eventos No Controlables, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.

9.3. Identificación de amenazas

Una amenaza se puede entender como los posibles eventos que nos pueden afectar negativamente en un futuro cercano.

Entre las entrevistas de levantamiento de información y visitas a las oficinas administrativas y a un grupo de establecimientos de salud del SISOL en Lima se identificaron las siguientes amenazas a los cuales se está expuesto los activos de información.

Categoría	Amenazas	Tipo	Origen
Eventos Naturales	Fuego	Controlable	Deliberado, accidental o ambiental
	Sismo	No Controlable	Ambientales
	Inundaciones a causa de desastres naturales	No Controlable	Deliberado, Accidental
Perdida de servicios esenciales	Aire acondicionado	Controlable	Deliberado, Accidental
	Perdida de Energía Eléctrica	No Controlable	Deliberado, Accidental
	Perdida de conectividad de red	Controlable	Deliberado, Accidental, Ambiental
Amenaza humanas	Robo de equipos	No Controlables	Deliberado
	Vandalismo	No Controlables	Deliberado
	Hacking (Denegación de Servicios)	No Controlables	Deliberado
	Robo de Información	Controlable	Deliberado
	Sabotaje	Controlable	Deliberado
Fallas Técnicas	Falla de hardware de cómputo y servidores	No Controlable	Accidental
	Falla de Sistemas de información y Software base	No Controlable	Accidental
Daño Físico	Aniegos	Controlable	Accidental
	Polvo, Corrosión	Controlable	Ambientales

9.4. Identificación de Vulnerabilidades

Una vulnerabilidad es una debilidad de un recurso informático o de un control, que puede ser aprovechada por una amenaza. Se trata de una característica negativa del recurso de información o de un control que se implementó sobre él, que lo hace vulnerable. En efecto, esa vulnerabilidad es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento.

A continuación, se listan las vulnerabilidades identificadas a partir de las amenazas encontradas. Es preciso indicar que una vulnerabilidad no causa daño, simplemente es una condición o conjunto de condiciones que pueden hacer que una amenaza afecte un activo informático.

Categoría	Cod.	Amenazas	Vulnerabilidad
Eventos Naturales	EN-001	Fuego	• Falta de equipo de detectores de humo en ambientes críticos y sensores de temperatura. • Falta de equipos de aspersión automática. • Falta de extintores de polvo químico en ambientes críticos.
	EN-002	Sismo	• Copias de backup en el mismo medio físico donde se registran.
	EN-003	Inundaciones a causa de desastres naturales	• Punto único de falla (único datacenter). • Cuartos de comunicaciones /gabinetes en establecimientos de salud expuestos al medio ambiente y lugares no adecuados.
Perdida de Servicios Esenciales	PS-001	Aire acondicionado	• No se dispone de equipos de aire acondicionado de precisión. • No se dispone de un sistema de alerta de temperatura y humedad en ambientes críticos.
	PS-002	Perdida de Energía Eléctrica	• Falta de energía estabilizada en los ambientes críticos, tanto en las sedes administrativas como en los establecimientos de salud. • Solo se cuenta con UPS en establecimientos de salud para los equipos críticos.
	PS-003	Perdida de conectividad de red	• No se dispone de una línea alterna de conectividad a internet. • Los establecimientos de salud no cuentan con una conexión dedicada a internet y se producen cortes o inestabilidad de la red. • El cableado de red no se encuentra con el entubado y canalizado adecuado en muchos establecimientos. • No se dispone de equipos de comunicaciones de backup.
Amenaza Humanas	AH-001	Robo de equipos	• Punto único de falla (Un solo datacenter). • Falta de copias de respaldo diario. • Falta de backup actualizado de todos los establecimientos de salud. • No se dispone de equipos de cómputo, de comunicaciones preparados para contingencias. • No se cuenta con cámara de video vigilancia en los ambientes críticos.
	AH-002	Vandalismo	• Punto único de falla (único datacenter). • Servidores no redundantes para aplicativos críticos. • Falta de backup actualizado de todos los establecimientos de salud. • Equipo servidores en los establecimientos de salud en sitios no adecuados y a la vista del público.
	AH-003	Hacking (Denegación de Servicios)	• Falta de políticas de seguridad de la información. • Falta de procedimientos de contingencia. • Falta de copias de respaldo diario. • Falta de equipos de comunicaciones adecuados para el control de acceso a internet y a la red de datos. • Falta de un control de software no controlado.
	AH-004	Robo de Información	• Falta de procedimientos de respaldo diario. • Falta de procedimientos de contingencia.

			• Falta de procesos de control de cambios y configuración. • Falta de un proceso para el resguardo de la información.
	AH-005	Sabotaje	• No se dispone de cámaras de seguridad ni control de acceso a ambientes críticos
			• Equipo servidores en los establecimientos de salud en sitios no adecuados y a la vista del público.
Fallas Técnicas	FT-001	Falla de hardware de cómputo y servidores	• Servidores configurados en baja disponibilidad. • Falta de backup actualizado de todos los establecimientos de salud. • No se dispone de servidores y equipos de contingencia establecidos. • Falta de control de cambios de la configuración de los equipos. • Falta de mantenimientos preventivos.
	FT-002	Falla de Sistemas de información y Software base	• Falta de políticas de desarrollo de software que permitan mantener un orden y ayude a identificar fallas. • Falta de control de versiones de software critico
Daño Físico	DF-001	Aniegos	• No se dispone de sensores de aniegos en el datacenter principal
	DF-002	Polvo, Corrosión	• Equipo servidores en los establecimientos de salud en sitios no adecuados

9.5. Análisis de Riesgos

El análisis del riesgo de EL PLAN se basa en la información generada en la fase de identificación de las vulnerabilidades y amenazas, que se convierten ahora en información para la toma de decisiones.

En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo; la probabilidad, el impacto y la exposición al riesgo. Estos elementos permitirán al Comité de Contingencias categorizar los riesgos, lo que a su vez le permitirá tomar diversas acciones ante los riesgos.

a. Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Así mismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

Para establecer la probabilidad de los eventos negativos que se pudieran presentar en la institución se utilizará la siguiente escala.

Escala de Probabilidad	
Calificación	**Explicación**
Muy improbable	10%, Remoto, puede ocurrir en circunstancias excepcionales
Improbable	25%, No esperado, pero podría ocurrir algunas veces
Moderado	50%, Se espera que ocurra regularmente
Probable	75%, Mayor, probable, se espera que ocurra
Casi Cierta	99%, Alta, certera

b. Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos o la magnitud de una pérdida causados. Es una calificación aplicada al riesgo para describir su impacto en relación al grado de afectación del servicio. Cuanto mayor sea el número, mayor es el impacto.

Escala de Impactos	
Calificación	**Explicación**
Insignificante	Sin perjuicios, perdida financiera asociada baja.
Menor	Perdida menor, costos financieros asociados bajos.
Moderado	Perdida moderada, no amenaza la imagen y confianza de institución.
Mayor	Mayor, pérdidas significativas financieras, amenaza la imagen y confianza de la institución.
Muy Significativo	Altas pérdidas financieras, pone en alto riesgo la imagen y confianza de la institución.

c. Exposición al Riesgo

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

d. Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán como se indica a continuación.

PROBABILIDAD	Fac	**Matriz de Riesgos**				
Casi Cierta	5	Moderado	Alto	Alto	Extremo	Extremo
Probable	4	Moderado	Moderado	Alto	Alto	Extremo
Moderado	3	Bajo	Moderado	Moderado	Alto	Alto
Improbable	2	Bajo	Bajo	Moderado	Moderado	Alto
Muy improbable	1	Bajo	Bajo	Bajo	Moderado	Moderado
Factor		1	2	3	4	5
		Insignificante	Menor	Moderado	Mayor	Muy significativo
		IMPACTO				

e. Valorización del Riesgo

De acuerdo a las definiciones de impacto y probabilidad se han valorizado los riesgos de las amenazas identificadas así como los posibles activos informáticos impactados. La información ha sido obtenida de las entrevistas

con el jefe de la USP, además de visitas a un grupo de establecimientos de salud.

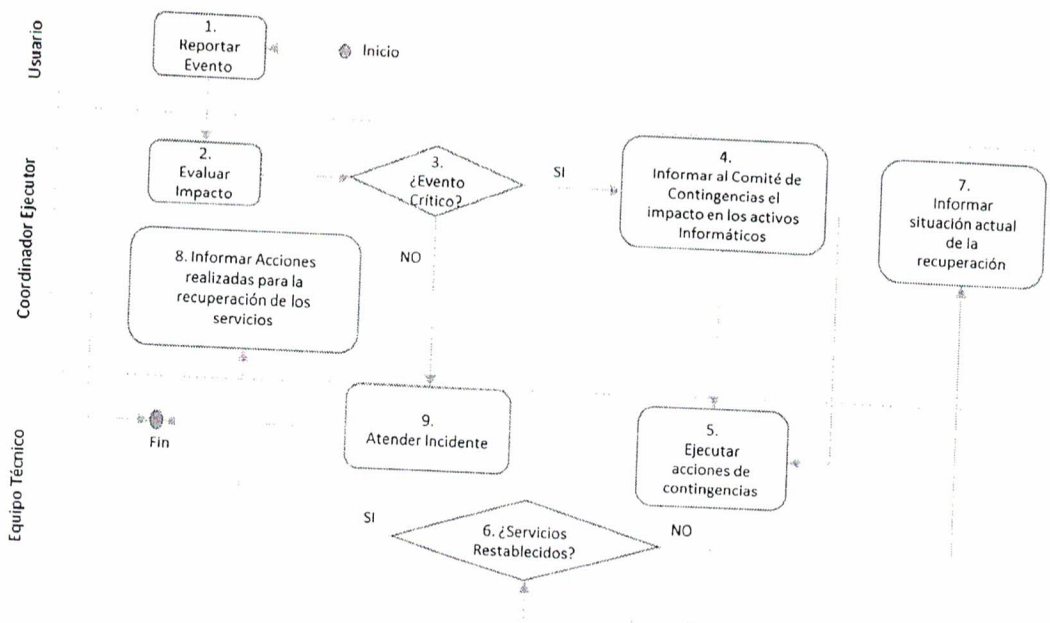
Categoría	Amenazas	Cod.	Activos informáticos	Prob. de ocurrencia	Impacto	Valor del riesgo
Eventos Naturales	Fuego	EN-001	Todos los elementos de los activos informáticos	4	5	Extremo
	Sismo	EN-002	Todos los elementos de los activos informáticos	4	5	Extremo
	Inundaciones a causa de desastres naturales	EN-003	Servidores, equipos de cómputo, cableado de red, tomas eléctricas, equipos UPS	2	3	Moderado
Perdida de Servicios Esenciales	Aire acondicionado	PS-001	Servidores, switches, routers	4	4	Alto
	Perdida de Energía Eléctrica	PS-002	Servidores, software, información, aire acondicionado, estaciones de trabajo	4	4	Alto
	Perdida de Conectividad de Red	PS-003	Servidores, software, información, impresoras, scanners	4	4	Alto
Amenaza Humanas	Robo de equipos	AH-001	Hardware, equipos de comunicaciones, UPS, logística operativa	3	4	Moderado
	Vandalismo	AH-002	Hardware, equipos de comunicaciones, UPS, logística operativa, servicios públicos, recursos humanos, otros equipos.	3	4	Moderado
	Hacking (Denegación de Servicios)	AH-003	Aplicativos utilizados por el SISOL, Bases de Datos	3	3	Moderado
	Robo de Información	AH-004	Base de Datos, respaldos de información	3	4	Moderado
	Sabotaje	AH-005	Software, servicios públicos	3	3	Moderado
Fallas Técnicas	Falla de hardware	FT-001	Servidores, equipos de cómputo, impresoras, escanners, equipos multimedia, switch, router.	3	5	Alto
	Falla de Sistemas de información y Software base	FT-002	Bases de datos, aplicativos informáticos, software de aplicaciones	4	5	Extremo
Daño Físico	Aniegos	DF-001	Servidores, equipos de cómputo, cableado de red, tomas eléctricas, equipos UPS	3	3	Moderado
	Polvo, Corrosión	DF-002	Servidores, equipos de cómputo, impresoras, scanner, lectores de código de barras, equipos multimedia, switchs, routers, anexos, UPS, aire acondicionado	3	3	Moderado

V°B° MARLON FALLA CASTRO JEFE USP Sistema

10. Procedimientos de Contingencia Informática

10.1. Proceso de Activación de EL PLAN

Una vez identificados los eventos de contingencia y los riesgos asociados, pasamos a desarrollar los procedimientos de recuperación y planes de acción en caso se concreten los riesgos. A manera de resumen, presentamos un flujo general que explica la forma de responder ante la ocurrencia de una contingencia.



N°	Actividad	Rol	Descripción
1	Reportar Evento	Usuario	Los usuarios del SISOL reportan la ocurrencia de una contingencia que interrumpa la normal operación de los servicios informáticos. En el caso de Sismos, incendio, inundaciones, robo de activos informáticos se reportará a la seguridad de la sede que está siendo afectada, el mismo que escalará a la Gerencia de Administración y Finanzas. En el caso estos eventos impacten en activos informáticos o se presenten virus, fallas de hardware, software y aplicaciones informáticas se reportará a las personas responsables de la USP.
2	Evaluar Impacto	Coordinador Ejecutor	El Coordinador Ejecutor identificará si la contingencia reportada es crítica y evalúa posibles impactos en los servicios informáticos.
3	¿Evento critico?	Coordinador Ejecutor	SI: Actividad 3 No: Actividad 9

4	Informar al Comité de Contingencias el impacto en los activos Informáticos	Coordinador Ejecutor	De acuerdo a la evaluación realizada por el Coordinador Ejecutor, este informará al Comité de Contingencias y se activarán los procedimientos de contingencia al verse los servicios informáticos afectados por el evento.
5	Ejecutar acciones de Contingencias	Equipo Técnico	El Coordinador Ejecutor pondrá en marcha acciones prioritarias para el restablecimiento de las operaciones críticas y la recuperación de los servicios tecnológicos.
6	¿Servicios restablecidos?	Equipo Técnico	SI: Actividad 8 No: Actividad 7
7	Informar situación actual de recuperación	Coordinador Ejecutor	El Coordinador Ejecutor informará al Comité de Contingencias las acciones realizadas para la recuperación de las operaciones y los resultados de los mismos, detallando los problemas presentados y las necesidades críticas para restablecer la operación.
8	Informar Acciones realizadas para la recuperación de los servicios al Comité de Contingencias	Coordinador Ejecutor	El Coordinador Ejecutor informará al Comité de Contingencias las acciones realizadas que se realizaron para el restablecimiento de las operaciones críticas y los tiempos de no disponibilidad.
9	Atender Incidente	Equipo Técnico	Si el evento reportado no ha afectado a los activos informáticos, el Coordinador Ejecutor atenderá el incidente con su equipo técnico.

10.2. Criticidad

La criticidad señala cuan crítico es un proceso, activo o servicio informático brindado por SISOL, así como el nivel de impacto del mismo. Se utilizará la siguiente clasificación:

- ✓ Crítico: El proceso, activo o servicio informático es altamente crítico, es decir no puede detenerse nunca y no deber ser interrumpido durante las horas de atención u operación.
- ✓ Importante: El proceso, activo o servicio informático puede ser suspendido por un breve lapso de tiempo no mayor a las 2 horas.
- ✓ No critico: El proceso, activo o servicio informático puede ser suspendido por un lapso de tiempo no mayor a 24 horas.

A continuación se presentan los valores de criticidad de los sistemas informáticos de negocio y operativos del SISOL, de acuerdo a la clasificación presentada:

N°	Nombre	Descripción	Criticidad
1	SIGHO	Sistema de Gestión Hospitalaria	Crítico
2	ZINCRON	Sistema de Control de Asistencia	Importante
3	Control Patrimonial	Sistema de Control Patrimonial	Importante
4	PERSON	Registro de Personal del SISOL	Importante

5	Web Service	Servicios de consulta de interconexión con los establecimientos de salud	Importante
6	Correo electrónico	Servicio de correo electrónico	Importante
7	Página Web	Página Web Institucional	No Critico

10.3. Estructura de los Planes de Contingencia

EL PLAN contemplan actividades antes, durante y después de ocurrido un desastre que afecte los servicios informáticos y las operaciones normales del SISOL.

Las acciones a ser consideradas en EL PLAN estarán dadas en una perspectiva del tiempo:

- ✓ *Antes*, como un plan de respaldo o de prevención para mitigar los incidentes o amenguar su impacto.
- ✓ *Durante*, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- ✓ *Después*, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

11. Desarrollo de los Planes de Acción

A continuación, se definen los planes de acción para los riesgos categorizados como Extremos y Altos, que han sido identificados en la sección anterior, los cuales se tomarán en cuenta para la atención de las contingencias y la recuperación de los servicios informáticos afectados por la ocurrencia de un desastre o fallas que interrumpan las operaciones del SISOL.

11.1. Eventos Naturales

11.1.1. Fuego (EN-001)

Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

a. Posibles Activos Informáticos Afectados

Este evento incluye los siguientes activos críticos identificados por SISOL vulnerables a causa de un incendio:

- ✓ Datacenter de la sede administrativa (servidores y equipos de comunicaciones).
- ✓ Cuartos de servidores de los establecimientos de salud (servidores y equipos de comunicaciones).
- ✓ Cableado de la red de datos.
- ✓ Recursos humanos (Personal capacitado para afrontar la contingencia.

b. Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones del SISOL, de verse afectadas, sin exponer la seguridad de las personas.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto muy significativo en los servicios informáticos y se identifica como un riesgo extremo.

d. Entorno

Este evento se puede dar en las instalaciones administrativas y los establecimientos de salud del SISOL, pudiendo afectar sus operaciones.

e. Personal Encargado

La Gerencia de Riesgos del SISOL y el Coordinador Ejecutor serán los que deberán dar cumplimiento a lo descrito en las condiciones de prevención de riesgo y los procesos de recuperación de las operaciones ante un incendio.

f. Plan de Prevención

- ✓ Verificar que los backups de información se estén realizando de manera oportuna y se encuentren actualizados.
- ✓ Verificar que el medio físico donde se encuentren los backups de información no se encuentren almacenarse en el mismo ambiente físico donde se registran.

- ✓ La Gerencia de Riesgos deberá realizar inspecciones de seguridad periódicamente y verificar que las rutas de escape se encuentren libres.

- ✓ Verificar que las conexiones eléctricas sean seguras y con toma a tierra.

- ✓ Solicitar a la Gerencia de Riesgos la realización de charlas sobre el uso y el manejo de los diversos tipos de extintores al personal.

- ✓ Acatar las indicaciones del INDECI en sus inspecciones relacionadas a incendios.

- ✓ Mantener visible en zonas cercanas al datacenter y cuartos de servidores una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, responsables de cómputo y soporte técnico de la USP.

- ✓ Verificar que los detectores de humo y sistemas de alarma en el datacenter y cuartos de comunicaciones se encuentren operativos ante un posible incendio.

- ✓ Coordinar con la Gerencia de Riesgos para la creación de brigadas antincendios con participación del personal del SISOL.

- ✓ Mantener actualizado los extintores (fecha de vencimiento vigente), y ubicarlos en zonas visibles y sin obstáculos.

MUNICIPALIDAD METROPOLITANA DE LIMA
V°B°
MARLON FALLA CASTRO
JEFE USP
Sistema Metropolitano de la Solidaridad

g. Plan de Ejecución

✓ Eventos que activan la de Contingencia

El proceso de contingencia se activará inmediatamente después de ocurrir el incendio y que tenga impacto en los servicios informáticos del lugar afectado.

✓ Personal que autoriza la contingencia

El Coordinador Ejecutor en primera instancia autorizará los procedimientos de recuperación o cualquier miembro del Comité de Contingencias de no encontrarse disponible el Coordinador Ejecutor.

✓ Actividades durante la contingencia

Las actividades que se describen a continuación podrán ser realizadas por el personal de la USP u otro que se encuentre en la zona del siniestro.

- Si el fuego está iniciando (amago) en el datacenter o cuarto de servidores, ubicar los extintores más cercanos e intentar apagar el fuego en la medida de lo posible. En ningún momento se debe echar agua sobre equipos electrónicos.

- De no ser posible controlar el siniestro debe evacuar el área y dar aviso a las demás oficinas, al personal de seguridad del lugar afectado y activar los sistemas de alarma que se dispongan.

- En todo momento coordinar con el personal de seguridad del lugar afectado para las acciones que deban de realizar.

✓ Actividades después del evento

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.

- En caso de daños del personal prestar asistencia médica inmediata.

- En caso se haya detectado bienes afectados a causa de la contingencia, se evaluará los daños en los activos informáticos para determinar la reposición o restauración de los mismo.

- El Coordinador Ejecutor junto con el Coordinador Logístico evaluarán las necesidades que se requieren para la habilitación de ambientes provisionales alternos, para restablecer las operaciones.

✓ Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio, recuperar los servicios informáticos hasta el restablecimiento total de los mismos en condiciones normales.

h. Plan de Recuperación

✓ Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la operatividad de los servicios informáticos interrumpidos.

El Coordinador Ejecutor y el equipo Técnico evaluaran si los activos informáticos han sufrido daños en el área afectada por el incendio y plantearan los procedimientos y necesidades urgentes para recuperar las operaciones del SISOL en el menor tiempo posible de ser necesarios.

- ✓ **Mecanismos de Recuperación**

El Coordinador Ejecutor informará al Comité de Contingencias las acciones y los tiempos de recuperación de los servicios informáticos que se hayan visto afectados, de acuerdo a las evaluaciones de daños realizadas después de ocurrido el incendio.

- ✓ **Desactivación del Plan de Contingencia**

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven a la recuperación de las operaciones informáticas en el lugar afectado.

- ✓ **Proceso de Actualización**

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir o amenguar el impacto de ocurrir un nuevo evento.

11.1.2. Sismos (EN-002)

Los sismos son movimientos en el interior de la tierra y generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno. Si bien es cierto, la ocurrencia de un sismo no se puede predecir, se deberán tomar las medidas que disminuyan su impacto en las personas, infraestructura, bienes y la operación de la institución.

a. Posibles Activos Informáticos Afectados

Este evento podría impactar en los siguientes activos informáticos críticos del SISOL, los mismos que podrían causar la contingencia en los servicios tecnológicos:

- ➢ Equipos Servidores y de comunicaciones en el datacenter de la sede administrativa y gabinetes de servidores en los establecimientos de salud.

- Cableado de la red de datos de las sedes administrativas.
- Personal especializado de la USP del SISOL.

b. Objetivo

Establecer las acciones que se tomarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones informáticas de la institución evitando exponer la seguridad de las personas.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto muy significativo en el servicio y se identifica como un riesgo extremo.

d. Entorno

Este evento se puede dar en las sedes administrativas y establecimientos de salud a nivel nacional del SISOL.

e. Personal Encargado de la Prevención

La Gerencia de Riesgos del SISOL y el Coordinador Ejecutor serán los que deberán dar cumplimiento a lo descrito en las condiciones de prevención de riesgo ante un sismo.

f. Plan de Prevención

- ✓ Verificar que los respaldos de información crítica se estén realizando de manera oportuna de acuerdo a los procedimientos establecidos.
- ✓ Verificar que las copias de respaldo no se encuentren almacenados en el mismo ambiente físico donde se registran los datos.
- ✓ La Gerencia de Riesgos deberá realizar inspecciones de seguridad periódicamente y verificar que las rutas de escape estén libres.
- ✓ La Gerencia de Riesgos deberá contar con un plan de evacuación de las instalaciones de cada sede administrativa y establecimientos de salud, el mismo que debe ser de conocimiento de todo el personal.
- ✓ La Gerencia de Riesgos deberá capacitar una brigada antisismos de entre el personal en todas las sedes del SISOL,

los cuales ayudaran a la evacuación de las personas de los locales afectados.

- ✓ Realizar simulacros de evacuación con la participación de todo el personal de las sedes administrativas y los establecimientos de salud.
- ✓ Mantener las rutas de escape libres de obstáculos en las sedes administrativas y establecimientos de salud.
- ✓ Señalizar todas las salidas en el datacenter o cuartos de servidores en las sedes administrativas y establecimientos de salud.
- ✓ Señalizar las zonas seguras en el datacenter o cuartos de servidores en las sedes administrativas y establecimientos de salud.
- ✓ Definir los puntos de reunión en caso de evacuación en las sedes administrativas y establecimientos de salud.
- ✓ Disponer en lugares visibles los números de emergencia.
- ✓ Mantener operativos los sistemas de alerta y evacuación en las sedes administrativas y establecimientos de salud.

g. Plan de Ejecución

✓ Evento que activa la Contingencia

Los procesos de contingencia se activarán inmediatamente después de ocurrir un sismo de regular intensidad o mayor.

✓ Personal que autoriza los procedimientos de contingencia

El Coordinador Ejecutor en primera instancia o cualquier miembro del Comité de Contingencias (de no encontrarse disponible el Coordinador Ejecutor) autorizarán la ejecución de los procedimientos de recuperación y planes de acción.

✓ Actividades durante la contingencia

- ➢ Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- ➢ Evacuar las oficinas de acuerdo a las disposiciones de la seguridad del local afectado, utilizando las rutas establecidas durante los simulacros. Considerar el uso de las escaleras de emergencia de existir, seguir la señalización de rutas de escape, zonas de agrupamiento

del personal, etc. Por ningún motivo utilizar los ascensores si se cuenta con ellos.

- Brindar los primeros auxilios al personal afectado si fuese necesario.

✓ Actividades después de Ocurrida la Contingencia

- El Coordinador Ejecutor conjuntamente con su equipo técnico evaluarán los daños ocasionados por el sismo sobre los ambientes del datacenter, gabinetes de comunicaciones, cableado de red, equipos de cómputo, servidores, instalaciones eléctricas, entre otros activos informáticos del local afectados.

- En caso la magnitud del sismo haya ocasionado daños a las estructuras del local afectado y a los ambientes donde se encuentre el datacenter y gabinetes de comunicaciones solicitará al Comité de Contingencias la presencia de personal especializado (ejemplo INDECI) realice una inspección y evaluación antes de ejecutar los procedimientos de recuperación de los servicios tecnológicos en el lugar afectado.

- Elaborar un inventario de los activos informáticos y servicios afectados, indicando el estado de operatividad de los mismos.

- El Coordinador Ejecutor junto con el Coordinador Logístico evaluará las necesidades que se requieren para la habilitación de ambientes provisionales alternos, para restablecer las operaciones.

✓ Duración

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas, los daños a la infraestructura y su recuperación.

h. Plan de Recuperación

✓ Descripción

El plan de recuperación estará orientado a restablecer en el menor tiempo posible la operatividad de los servicios informáticos interrumpidos.

El personal encargado de ejecutar los procedimientos de recuperación de los servicios informáticos afectados es el Coordinador Ejecutor conjuntamente con su equipo técnico.

V°B° MARLON FALLA CASTRO JEFE USP Sistema Municipalidad de la Solidaridad

✓ Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias las acciones y los tiempos de recuperación de los servicios informáticos que se hayan visto afectados, de acuerdo a las evaluaciones de daños realizadas después de ocurrido el sismo.

✓ Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven a la recuperación de las operaciones informáticas en el lugar afectado.

✓ Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir o amenguar el impacto de ocurrir un nuevo evento.

11.2. Pérdida de Servicios Esenciales

Con el fin de mantener las condiciones ambientales precisas para la integridad de los servidores, los sistemas de información y datos los datos almacenados en estos, es indispensable un sistema de regulación de temperatura que controle los niveles de calor y humedad en los ambientes del datacenter y cuartos de servidores.

Si un servidor se sobrecalienta, se reduce su capacidad de transferir calor, por lo que este se absorbe en sus mismos componentes y se sobrecalienta aún más. Este proceso ocurre en periodos de tiempo muy cortos. Un sobrecalentamiento puede además activar protecciones propias del equipo de cómputo que lo lleva a apagarse y proteger así la integridad de la unidad, poniendo en riesgo la continuidad del negocio.

11.2.1. Aire acondicionado (PS-001)

a. Posibles Activos Informáticos Afectados

Este evento podría impactar en los siguientes activos informáticos críticos del SISOL

- ✓ Servidores.
- ✓ Equipos de comunicaciones.

- ✓ Datos.
- ✓ Sistemas de información.

b. Objetivo

Establecer las acciones que se tomarán ante una falla (interrupción) del equipo de aire acondicionado del datacenter o cuartos de servidores a fin de evitar el sobrecalentamiento y daño de los equipos informáticos críticos.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto mayor en el servicio y se identifica como un riesgo alto.

d. Entorno

Este evento se puede dar en el datacenter y cuartos de servidores en las sedes administrativas o establecimientos de salud del SISOL que dispongan de estos ambientes.

e. Personal Encargado

El Coordinador Ejecutor y su equipo técnico será el que dé cumplimiento a lo descrito en las condiciones de prevención y planes de ejecución ante una pérdida de aire acondicionado.

f. Plan de Prevención

- ✓ Implementar equipos de aire acondicionado de precisión en el datacenter. De ser posible, disponer de un equipo de contingencia.
- ✓ Identificar un lugar adecuado para la instalación de los equipos de aire acondicionado a fin de que el aire frio se distribuya uniformemente.
- ✓ Implementar un plan de mantenimientos preventivos de los equipos de aire acondicionado del datacenter y cuartos de servidores.
- ✓ Verificar no existan fugas de aire frío de los ambientes del datacenter y cuartos de servidores.
- ✓ Contar grupos grupo electrógeno de contingencia disponible para cortes de energía eléctrica que afecten el funcionamiento de los equipos de aire acondicionado.

- ✓ Implementar equipos detectores de temperatura y humedad con capacidad de monitoreo y envío de alertas en el datacenter y cuartos de servidores.

- ✓ Tener disponibles los teléfonos de emergencia del proveedor de soporte técnico de los equipos de enfriamiento.

g. Plan de Ejecución

✓ Eventos que activan la Contingencia

El evento que activa la contingencia es cuando deja de funcionar el equipo de aire acondicionado del datacenter en la sede principal o del cuarto de comunicaciones en los establecimientos de salud. El proceso de contingencia se activará inmediatamente después de ocurrir el evento y se activen las alarmas de temperatura.

✓ Personal que autoriza la contingencia

El Coordinador Ejecutor autorizará la ejecución de los procedimientos de recuperación.

✓ Actividades Durante la Contingencia

- ➢ Los sensores de temperatura y humedad deberán de alertar, mediante una alarma sonora, cuando detecta valores de temperatura y humedad superiores a los permitidos.

- ➢ Comunicar a la USP o al encargado de cómputo para su revisión y escalamiento.

- ➢ El personal encargado de la USP verificará el funcionamiento del equipo de aire acondicionado.

- ➢ El personal encargado tomará los valores de temperatura y humedad del datacenter o cuartos de comunicaciones.

- ➢ De ser necesario reportar el caso al soporte técnico del equipo de aire acondicionado.

- ➢ El Coordinador Ejecutor podrá solicitar al Coordinador Logístico la instalación y operación de un equipo de aire acondicionado alterno para el datacenter o establecimiento de salud.

✓ Duración

La duración total del evento se dará mientras no se restablezca el funcionamiento normal del equipo de aire acondicionado.

h. Plan de Recuperación

✓ Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias en caso se presentara corte en los servicios o equipos afectados por el evento, así como las acciones realizadas, los tiempos de recuperación y las necesidades de adquisición de otro equipo, si fuera el caso.

✓ Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven a la recuperación de las operaciones informáticas en el lugar afectado.

✓ Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir futuros eventos o amenguar su impacto.

V°B°
MARLON
FALLA CASTRO
JEFE

11.2.2. Pérdida de Energía Eléctrica (PS-002)

Un corte de energía eléctrica es la pérdida del suministro de energía eléctrica en un área. La razón para la caída del suministro normalmente podría estar en el fallo de alguno de los elementos que componen el sistema de suministro eléctrico, por ejemplo, un defecto de la subestación eléctrica, daños en una línea eléctrica (accidentales o intencionados), o en otra parte del sistema de distribución, un cortocircuito, una sobrecarga o, incluso, un error humano en la operación sobre elementos del sistema.

a. Posibles Activos Informáticos Afectados

- ✓ Servidores
- ✓ Equipos de comunicaciones
- ✓ Equipos de cómputo
- ✓ Sistemas de información

b. Objetivo

Establecer las acciones que se tomarán ante una interrupción de la energía eléctrica del datacenter o cuartos de servidores a fin de minimizar el tiempo de interrupción de los equipos críticos.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto mayor en el servicio y se identifica como un riesgo alto.

d. Entorno

Este evento se puede dar en las sedes administrativas y establecimientos de salud, el datacenter y cuartos de servidores en las sedes administrativas o establecimientos de salud del SISOL que dispongan de estos ambientes.

e. Personal Encargado

El Coordinador Ejecutor y su equipo técnico serán los que den cumplimiento a lo descrito en las condiciones de prevención y planes de acción ante una pérdida de la energía eléctrica.

f. Plan de Prevención

- ✓ Implementar en los ambientes del datacenter y cuartos de servidores Sistemas de alimentación ininterrumpida (UPS) que soporten una continuidad de funcionamiento de los equipos servidores críticos.
- ✓ Disponer de un grupo electrógeno capaz de soportar la carga del datacenter o establecimientos de salud cuando lo requieran.
- ✓ Verificar el pozo a tierra del datadenter o cuartos de servidores cuenten con los mantenimientos preventivos adecuados.
- ✓ Verificar si la carga eléctrica disponible en el datacenter o cuartos de servidores soporten la instalación de nuevos equipos.
- ✓ Disponer de linternas en los ambientes del datacenter y cuartos de servidores, así como luces de emergencia.
- ✓ Tener a la mano los números de emergencia de la empresa proveedora de energía eléctrica.

V°B°
MARLON FALLA CASTRO
JEFE USP

- ✓ Implementar equipos de estabilización de energía eléctrica a los cuales se deberán conectar los equipos de cómputo.
- ✓ Establecer los tiempos de espera máximos para aplicar la contingencia eléctrica si no se dispone de un sistema automático de generadores de energía.
- ✓ Verificar periódicamente el funcionamiento de las baterías de los equipos UPS, especialmente los que alimentan a equipos críticos.
- ✓ Coordinar la instalación y funcionamiento de un grupo electrógeno con el Coordinador Logístico en las sedes administrativas o establecimientos de salud que puedan verse afectados por un corte de energía eléctrica programado.
- ✓ Coordinar con las áreas usuarias procedimientos operativos alternos para los casos de falla de los sistemas informáticos, de tal manera que no se afecte la atención.

g. Plan de Ejecución

✓ Eventos que activan la de Contingencia

El evento que activa la contingencia es cuando se corta de manera imprevista el fluido eléctrico en las sedes administrativos o establecimientos de salud que afecte los servicios informáticos.

✓ Personal que autoriza la contingencia

El Coordinador Ejecutor autorizará la ejecución de los procedimientos de recuperación.

✓ Actividades durante la contingencia

- ➢ En caso el corte de energía eléctrica sea inesperado y vaya a exceder el tiempo que soportan los equipos UPS (30 min aprox.) en el datacenter y cuartos de servidores, el encargado de soporte o analistas de sistemas procederán al apagado de los equipos de manera manual. Se deberá de informar al Coordinador Ejecutor de EL PLAN sobre esta acción.
- ➢ De no tener un tiempo de recuperación establecido por la empresa de proveedora de energía eléctrica, El Coordinador Ejecutor deberá de solicitar al Coordinador de Logístico la instalación de un equipo generador de energía eléctrica en el menor tiempo posible.

- El Coordinador Ejecutor, comunicará al Comité de Contingencias sobre la ocurrencia del incidente y las acciones tomadas.

✓ Duración

La duración total de la contingencia se dará mientras no se restablezca el fluido eléctrico en el lugar afectado.

h. Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias que parte de los servicios o equipos se han visto afectados, así como las acciones realizadas para su recuperación, los tiempos de recuperación y las necesidades de adquisiciones de emergencia si fuera el caso.

i. Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven al restablecimiento de la energía eléctrica.

j. Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir futuros eventos o amenguar su impacto y actualización de EL PLAN.

11.2.3. Pérdida de Conectividad de Red (PS-003)

Una red de área local (Local Area Network, o LAN) es un grupo de equipos de cómputo y dispositivos asociados que comparten una línea de comunicación común o un enlace inalámbrico con un servidor. Normalmente, una LAN abarca computadoras y periféricos (impresoras, scanners, etc.) conectados a un servidor dentro de un área geográfica distinta, como una oficina o un establecimiento comercial. Las computadoras y otros dispositivos móviles utilizan una conexión LAN para compartir recursos como una impresora o un almacenamiento en red para los datos.

Una red de área local puede servir no solo a dos o tres usuarios (por ejemplo, en una red de oficina pequeña), sino también a varios cientos de usuarios en diferentes ubicaciones físicas. Las redes LAN incluyen cables, conmutadores, enrutadores y otros componentes que permiten a los usuarios conectarse a servidores internos, sitios web y

otras redes LAN a través de redes de área extensa (WAN), mediante el uso del internet.

a. Posibles Activos Informáticos Afectados

- ✓ Equipos de comunicaciones (routers, switches, firewalls, patch panel, etc.)
- ✓ Infraestructura de red.

b. Objetivo

Establecer las acciones que se tomarán ante una falla de conectividad de red en los establecimientos de salud o sedes administrativas y la comunicación entre estas mediante los servicios de internet.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto mayor en el servicio y se identifica como un riesgo alto.

d. Entorno

Este evento se puede dar en las sedes administrativas y establecimientos de salud.

e. Personal Encargado

El Coordinador Ejecutor y su equipo técnico serán los que dé cumplimiento a lo descrito en las condiciones de prevención y planes de ejecución.

f. Plan de Prevención

- ✓ Toda implementación de cableado de red deberá ser tipo Categoría 6, evitando mezclar categorías de cable ya que degrada la velocidad de transferencia.
- ✓ Evitar el encadenamiento en cascada de switches, ya que en cada nivel la calidad de transferencia se degrada y no permitirá una rápida identificación de un punto de falla.
- ✓ Instalar los equipos de comunicaciones dentro de gabinetes de comunicaciones, rack de servidores, ubicándolos en lugares cerrados y de acceso sólo al personal de la USP.
- ✓ El tendido del cableado deberá estar debidamente canalizados mediante canaletas, ductos o bandejas pasa

cables adosados a las paredes o techos desde los switches de distribución a los puntos terminales.

- ✓ Se deberá contar con equipos de comunicaciones de backup para el recambio en caso no pueda ser recuperada su operatividad.

- ✓ Considerar la cantidad de usuarios, distancia del switch core y la tasa de transferencia total que se utilizará en una determinada área a cubrir con puntos de red, con el fin de determinar las características de los equipos a instalar y la tecnología de transferencia a considerar.

- ✓ Las terminales de los puntos de red deberán estar en cajas tomadatos debidamente identificados en ambos extremos (punto de red y terminal en patch panel).

- ✓ Se deberá llevar un registro de la ubicación física de los puntos de red y los equipos de comunicaciones conectados que permita identificar rápidamente los equipos conectados, administrando los cambios que se requieran.

- ✓ La red deberá estar segmentada de acuerdo a las necesidades del negocio, lo que permitirá evitar la saturación de la red para las necesidades críticas.

- ✓ La USP deberá definir y administrar los perfiles de red mediante IP, definiendo reglas de acceso en el firewall.

- ✓ El acceso a internet deberá de administrarse de acuerdo a las necesidades del negocio. Se recomienda para el datacenter contratar un segundo proveedor de internet de menor velocidad que se use como contingencia en caso de caídas.

- ✓ Se debe disponer de equipos de internet inalámbrico para dar soporte a los aplicativos críticos ante posibles caídas del servicio de internet fijo en los establecimientos de salud en lugares alejados.

- ✓ Utilizar en la medida de lo posible conexiones tipo VPN para la transmisión de la información entre todas las sedes del SISOL.

V°B° MARLON FALLA CASTRO JEFE USP Sistema Metropolitano de la Solidaridad

g. Plan de Ejecución

- ✓ Eventos que activan la de Contingencia

El evento que activa la contingencia se produce cuando se detecta la caída masiva de la red o internet que impida la utilización de servicios yo aplicativos críticos.

✓ Personal que autoriza la contingencia

El Coordinador Ejecutor autorizará la ejecución de los procedimientos de recuperación.

✓ Actividades durante la contingencia

- En caso el corte de red se deberá comunicar al personal de soporte técnico o encargado de cómputo, quienes evaluarán el incidente reportado.
- De no poder resolver el incidente, este deberá ser escalado al personal especializado de la USP para la evaluación del incidente.
- De ser necesario, se deberá hacer pruebas en campo para identificar el origen del problema. Si el origen del problema es por un equipo de comunicaciones, se deberá cambiar el equipo por otro de backup. Si el origen es el cableado de red, se deberá remplazar por otro provisional.
- Identificar si se han hecho cambios en la configuración de los equipos de comunicaciones o instalaciones de cableado de red.
- Si el incidente resulta un corte en el servicio de internet que afecte los servicios informáticos críticos se deberá reportar al proveedor de internet. De no resolverse el incidente dentro de 15 min a 30 min se procederá a configurar el canal secundario que se disponga o proporcionar un equipo de internet inalámbrico.

✓ Duración

La duración total de la contingencia se dará mientras no se restablezca el servicio regular de internet o la conectividad de la red local en el lugar afectado.

h. Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias que parte de los servicios o equipos se han visto afectados, así como las acciones realizadas para su recuperación, los tiempos de recuperación y las necesidades de adquisiciones de emergencia si fuera el caso.

i. Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven al restablecimiento del internet o la red local.

j. Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir futuros eventos o amenguar su impacto y la actualización de EL PLAN.

11.3. Fallas Técnicas

11.3.1. Falla de Hardware (FT-001)

Los equipos de cómputo, equipos de comunicaciones y servidores físicos están diseñados para cumplir requisitos determinados dentro de una red empresarial y tienen un ciclo de vida específico que comienza desde la adquisición, administración y su baja del servicio. En ese sentido, su administración y mantenimiento resulta muy importante para mantener su vida útil y los niveles de operación que estos soportan.

a. Posibles Activos Informáticos Afectados

- ✓ Servidores Físicos
- ✓ Equipos de computo
- ✓ Equipos de comunicaciones

b. Objetivo

Establecer las acciones que se tomarán ante una falla de hardware de equipos que impidan la operación de los servicios informáticos críticos.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto muy significativo en el servicio y se identifica como un riesgo alto.

d. Entorno

Este evento se puede dar en las sedes administrativas y establecimientos de salud donde se encuentren equipos servidores físicos, equipos de cómputo y de comunicaciones que den soporte a servicios críticos.

e. Personal Encargado

El Coordinador Ejecutor y su equipo técnico serán los que dé cumplimiento a lo descrito en las condiciones de prevención y planes de ejecución.

f. Plan de Prevención

- ✓ El Coordinador Ejecutor deberá mantener un listado de todos los equipos servidores físicos, sus ubicaciones, los sistemas operativos que soportan (si están virtualizados), los servicios que estos soportan, las credenciales de acceso y sus direcciones IP.

- ✓ El Coordinador Ejecutor deberá planificar e implementar mantenimientos preventivos a los equipos informáticos. Se sugiere para equipos servidores físicos se realicen mantenimientos preventivos 1 vez al año y para equipos de cómputo de 1 a 3 veces al año dependiendo las condiciones de operación.

- ✓ Los equipos servidores físicos deberán estar instalados en lugares acondicionados con aire acondicionado o ventiladores y de acceso restringido al personal autorizado. Así mismo, deberán estar conectados a fuentes de energía eléctrica estabilizada y UPSs. En el caso de los equipos de cómputo, estos deben de estar conectados por lo menos a corriente estabilizada y con tomas a tierra.

- ✓ Se debe considerar como una buena práctica para los servidores físicos que soportan procesos críticos tener un servidor alterno o de backup.

g. Plan de Ejecución

- ✓ Eventos que activan la de Contingencia

El evento que activa la contingencia se produce cuando se detecta la falla de un de un equipo servidor físico a raíz de una caída de un o varios servicios críticos soportados.

- ✓ Personal que autoriza la contingencia

El Coordinador Ejecutor autorizará la ejecución de los procedimientos de recuperación.

✓ Actividades durante la contingencia

- El Coordinador Ejecutor y su equipo técnico deberán evaluar el impacto en los servicios críticos impactados por la caída del hardware e informará al Comité de Contingencias las acciones y tiempo de recuperación de los servicios.
- En caso se dispongan de equipos de backup de similares características el Coordinador Ejecutor dispondrá las acciones necesarias para su instalación, configuración y puesta en operación.
- En caso se tenga configurado un servidor de respaldo se apuntará hacia este para que se continúe con la atención.
- El Coordinador Ejecutor podrá solicitar al Comité de Contingencias facilidades para el desplazamiento del personal especializado de la USP para recuperar la operatividad normal de los servicios críticos.

✓ Duración

La duración total de la contingencia se dará mientras no se restablezcan los equipos afectados que soporten de internet o la red local en el lugar afectado.

h. Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias que parte de los servicios o equipos se han visto afectados, así como las acciones realizadas para su recuperación, los tiempos de recuperación y las necesidades de adquisiciones de emergencia si fuera el caso.

i. Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven al restablecimiento normal del hardware averiado.

j. Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir futuros eventos o amenguar su impacto y la actualización de EL PLAN.

11.3.2. Falla de Sistemas de información y Software base (FT-002)

La creciente complejidad de los sistemas de información al integrar todos los procesos de negocio hace que estos puedan producir algún tipo de falla en su funcionamiento. Unos adecuados procesos de gestión de pruebas durante su implementación ayudarán a aumentar la calidad de un producto software.

a. Posibles Activos Informáticos Afectados

- ✓ Sistemas de información

b. Objetivo

Establecer las acciones que se tomarán ante una falla de los sistemas de información críticos.

c. Riesgo

El SISOL determina que el presente evento tiene un nivel de impacto muy significativo en el servicio y se identifica como un riesgo extremo.

d. Entorno

Este evento se puede dar en las sedes administrativas y establecimientos de salud donde se ejecuten servicios informáticos críticos.

e. Personal Encargado

El Coordinador Ejecutor y su equipo técnico serán los que dé cumplimiento a lo descrito en las condiciones de prevención y planes de ejecución.

f. Plan de Prevención

- ✓ Implementar una metodología estándar para el desarrollo de software en el SISOL, el cual contemple estándares para la programación y procedimientos de pruebas.
- ✓ Disponer de la documentación de las versiones de los aplicativos informáticos en producción tanto de los desarrollados por el SISOL como los adquiridos por terceros.
- ✓ Los cambios y/o actualizaciones solicitados a la USP de los sistemas informáticos deberán ser revisados por los

Analistas de Sistemas del SISOL y documentados adecuadamente.

- ✓ En caso de aplicativos desarrollados por terceros, contar con contratos de soporte vigente ante alguna contingencia.
- ✓ Contar con una base de datos del conocimiento donde se registren las fallas y las soluciones aplicadas que resolvieron una incidencia reportada en un aplicativo o sistema informático.
- ✓ Evaluar si las actualizaciones de los sistemas operativos podrían ser incompatibles con los sistemas usados por los usuarios.
- ✓ Coordinar con las áreas responsables del uso de los aplicativos procedimientos alternos de operación ante la no disponibilidad de aplicativos informáticos críticos ante una contingencia.
- ✓ Mantener las licencias de operación vigentes de los sistemas operativos y aplicativos informáticos de terceros.

g. Plan de Ejecución

✓ Eventos que activan la de Contingencia

El evento que activa la contingencia se produce cuando se detecta reporta una falla masiva en algún sistema de información crítico del SISOL e interrumpe las operaciones.

✓ Personal que autoriza la contingencia

El Coordinador Ejecutor autorizará la ejecución de los procedimientos de recuperación.

✓ Actividades durante la contingencia

- ➢ Los usuarios deberán dar aviso a la USP de la falla del sistema.
- ➢ El personal de Soporte Técnico o Encargado de Computo revisarán el problema presentado y coordinará con los Analistas de Sistemas la solución.
- ➢ En caso los sistemas que están afectados tengan procedimientos alternos de operación el Coordinador Ejecutor consultará con el área responsables para pasar a ese modo mientras se recupera el servicio.

V°B°
MARLON FALLA CASTRO
JEFE USP

✓ Duración

La duración total de la contingencia se dará mientras no se restablezcan los sistemas que estén presentando fallas.

h. Mecanismos de Recuperación

El Coordinador Ejecutor informará al Comité de Contingencias que parte de los servicios se han visto afectados, así como las acciones realizadas para su recuperación, los tiempos de recuperación y las necesidades de adquisiciones de emergencia si fuera el caso.

i. Desactivación del Plan de Contingencia

El Comité de Contingencias desactivará EL PLAN una vez que se haya tomado las acciones que lleven al restablecimiento normal del sistema que ha fallado.

j. Proceso de Actualización

El proceso de actualización de EL PLAN se realizará en base al informe presentado por el Coordinador Ejecutor, luego de lo cual se determinará las acciones a tomar para prevenir futuros eventos o amenguar su impacto.

12. Definición y ejecución del plan de pruebas

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento, y por ende convertirse en un problema prioritario de atender si éste se produjera en el horario de oficina que pueda resultar impactante durante las actividades del SISOL; es que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia y tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura.

En este sentido, la garantía del "éxito" del Plan de Contingencia se basa en una validación y certificación anticipada del mismo, en cada uno de sus procesos.

12.1. Alcance y Objetivos

Dado que la mayor parte de los planes de contingencia están orientados a temas de Siniestros, Seguridad y Recursos Humanos, cuyas situaciones son imposibles de reproducir en la vida real (Ej.: terremotos, robos, accidentes, problemas logísticos, etc.), es que el plan de pruebas estará enfocado principalmente a simular situaciones de contingencia en caso de

incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

En este contexto previo, podemos precisar los siguientes objetivos a alcanzar en la realización de las pruebas:

- ✓Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte de EL PLAN respecto a una posible interrupción de los procesos identificados como críticos para el servicio del SISOL.

- ✓ Identificar por medio de la prueba, las posibles causas que puedan atentar contra su normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).

- ✓Determinar los roles y funciones que cumplirán los responsables en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por un grupo determinado de usuarios de las diferentes direcciones y jefaturas del SISOL, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir EL PLAN.

V°B° MARLON FALLA CASTRO JEFE (e) Sistema de la Solidaridad

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- ✓OBJETIVOS DE LA PRUEBA
  - ➢ Definición Objetivos

- ✓ALCANCES
  - ➢ Áreas Afectadas (relación)
  - ➢ Personal involucrado (relación)

- ✓DESCRIPCIÓN DE LA PRUEBA A EFECTUARSE
  - ➢ Evaluación de una situación de Emergencia
  - ➢ Medios disponibles para operar
  - ➢ Fechas y horas.

- ✓RESULTADOS ESPERADOS DE LAS PRUEBAS Relación de posibles acciones.

12.2. Validación y Registro de Pruebas

Todas las actividades generales que forman parte de la prueba, deberán validarse, registrarse (incluyendo observaciones) y firmarse por todos los responsables que participaron en cada una de ellas, a fin de dar fe de su ejecución y certificación. En el Anexo A01 "Control y Certificación de Pruebas de Contingencia" se muestra el formato que se usará para la validación y registro de dichas pruebas, así como el detalle de la información que deberá ser ingresada en cada campo.

13. Disposiciones Finales

- ✓ EL PLAN deberá contar con el apoyo correspondiente por parte de la alta dirección, para suministrar de recursos financieros, humanos y materiales a fin de su implementación y ejecución.

- ✓ Los gerentes, jefes, y colaboradores que laboren en SISOL, deben tomar parte de las actividades y están obligados a participar en la implementación y ejecución de EL PLAN según corresponda a la emergencia presentada.

- ✓ El Comité de Contingencias deberá velar que el plan se cumpla cada vez que presente una contingencia que interrumpa la normal operación del SISOL.

- ✓ La USP debe definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento EL PLAN.

- ✓ Implementar un plan de capacitación y entrenamiento a todos los colaboradores del SISOL, con la finalidad afrontar situaciones de emergencia a través de charlas periódicas. El personal especializado de la USP deberá estar debidamente entrenado para prevenir y enfrentar cualquiera de los riesgos descritos en EL PLAN.

- ✓ Se debe difundir a todas las áreas del SISOL copias de EL PLAN, documentos resumen, carteles, afiches u otro tipo de documento para su información.

- ✓ Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan.

ANEXOS

A01: "Control y Certificación de Pruebas de Contingencia"

Codigo Nº: (del plan)

Control y Certificacion de Pruebas de Contingencia

Proceso en Prueba: (Nombre del proceso a probar/certificar)

Area responsable: (Area responsable del proceso probado/certificado)

Fecha: / / Hora Inicio: Hora Fin: (de prueba)

Informacion del Proceso

Metodologia y Alcance: (Que se va a hacer en la prueba y hasta donde va a abarcar la misma)

Condiciones de Ejecucion:

Equipo: (Nombre de equipo/s en la/s que se procesa la prueba/certificacion)

Aplicación Software: Version:

Fecha de Backup:

De la Prueba/ Certificacion

Resultado de la Prueba:

Satisfactorio: Satisfactorio con Observaciones: Deficiente:

Observaciones: (en el caso de haber observaciones o que la prueba haya sido deficiente se enlistaran los motivos de dichas deficiencias, así como resultados de las pruebas en todos los casos)

Actualizacion del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia: (Se indicarán los cambios que se realizarán en el Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

Participantes V° B° y Aprobación

Participante	Cargo	Firma