

 MINISTERIO de SALUD SNIS-VE	PLAN DE CONTINGENCIAS UNIDAD:SISTEMA NACIONAL DE INFORMACION EN SALUD Y VIGILANCIA EPIDEMIOLOGICA SNIS-VE PROYECTO: SOFTWARE DE ATENCIÓN PRIMARIA EN SALUD SOAPS	FORM/PC-01
---	---	---

a) Introducción

Siguiendo una política de continuidad en la atención a la población en general y la atención al paciente, el presente documento contiene las medidas técnicas y humanas necesarias para garantizar las posibles contingencias tecnológicas en los establecimientos de salud.

Se tiene conciencia de que no es posible eliminar todos los riesgos de pérdida total o parcial de los problemas, sin embargo, con la elaboración del presente plan es posible proponer métodos preventivos contra riesgos, minimizar el impacto al mínimo.

b) Definiciones

Plan de Contingencia. - Estrategia planificada con una serie de procedimientos que faciliten u orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la sociedad ante la eventualidad de todo lo que la pueda paralizar, ya sea de forma parcial o total.

Amenaza. - Cualquier cosa que pueda interferir con el funcionamiento adecuado de los sistemas. Ejemplo: Fallas de suministro eléctrico, virus o usuarios descuidados.

Incidente. - Cuando se materializa un problema, como por ejemplo las fallas de suministro eléctrico.

c) Objetivo

Proporcionar a la población en general un plan de contingencias, que contenga los procedimientos necesarios para minimizar el impacto de los hechos imprevistos, reanudando con la mayor brevedad posible la recuperación de los servicios, recursos y registros afectados en los diferentes niveles de gestión de la información.

d) Alcance

El presente plan se aplica a todos los niveles de gestión de la información en salud, que hagan uso de los sistemas informáticos proporcionados por el Ministerio de Salud a través del Sistema Nacional de Información en Salud y Vigilancia Epidemiológica SNIS-VE.

e) Definiciones de Procesos Críticos

En este acápite se realiza la definición de los procesos críticos (riesgos tecnológicos) que ocasionan que los servicios provistos por el sistema se vana interrumpidos, mismos que tendrían que ser cubiertos por el plan de contingencias.

Se realizo un análisis evento-causa para definir los riesgos mas críticos para el personal de salud, detallado a continuación:



Fallas de Hardware(Personal)	Vulnerabilidades y causas probables identificadas en el Análisis de Riesgo Tecnológico que afecta a los equipos de computación	Imposibilita el proceso de registro de las atenciones que dependen directamente del personal de salud del establecimiento.
Fallas de Software(Personal)	Vulnerabilidades y causas probables identificadas en el Análisis de Riesgo Tecnológico que afecta a los equipos de computación	Imposibilita de ejecutar con el proceso o las actividades críticas que dependen directamente del correcto funcionamiento de los recursos de hardware asignado al personal de salud del establecimiento.
Fallas en la red de Comunicaciones	Vulnerabilidades y causas probables identificadas en el Análisis Tecnológico	Imposibilitar el ejecutar el proceso o actividades críticas que dependen directamente de los recursos de la red de comunicaciones

f) Detalle de procesos críticos relevados

A continuación, se detallan los procesos críticos que ocasionarían interrupciones en el proceso normal del funcionamiento de las operaciones y/o prestación de servicios.

- Falla total o parcial del equipo destinado como servidor de Base de Datos que es utilizador por el sistema SOAPS, este puede ocurrir por algún factor personal interno o externo que afecte el correcto funcionamiento del hardware p software base donde se aloja la base de datos, debido a factores de manejo, actualizaciones aplicadas, factores externos, inestabilidad de energía eléctrica, falta de mantenimiento preventivo, entre otras, que presentes el efectivo funcionamiento del sistema o accesibilidad al mismo, al ignorar estas medidas puede generar riesgos de perder parcial o totalmente la información.
- Falta de Actualización del aplicativo (Base de Datos y Aplicación del SOAPS) y falla de equipos de computación, el hecho de no manejar de forma sincronizada las últimas versiones de los aplicaciones, bases de datos y además de manera sincronizada, puede ocasionar que el usuario final pueda generar fallas en el manejo y carga de datos, motivo por el cual puede dejar de utilizar el sistema o introducir información errónea, acciones que pueden a la larga generar una base de datos inconsistente y no confiable.
- Falla total o parcial de la red de comunicaciones, que impide el tráfico de datos desde los clientes al servidor, este puede ocurrir en todos los equipos conectados a la red o solamente en algunos usuarios finales.

g) Escenarios Previstos en caso de Contingencias

Para poder superar las contingencias anteriormente mencionadas se detallan a continuación las opciones que se deben aplicar para brindar continuidad de los servicios de información y minimizar el riesgo de pérdida de información.



Falla total o parcial del equipo destinado como servidor de Base de Datos que es utilizado por el sistema SOAPS. Para restablecer los servicios del gestor de base de datos del software base del servidor, necesarios para el funcionamiento del sistema SOAPS, se deben seguir los siguientes pasos:

- a. Se realiza el diagnostico del problema en el Servidor (hardware/software), se quite al equipo servidor de la red.
- b. En caso de tener problemas de software, servicios o actualizaciones se procede a reiniciar el equipo y levantar todos los servicios de manera correcta.
- c. Si alguna de las bases de datos presenta problemas de inicio, se procede a aplicar los procedimientos de recuperación de la base de datos o puesta en modo emergencia, esto para poder generar una copia de seguridad para su posterior proceso de recuperar la data en una nueva base de datos.
- d. Si con todo lo anterior no llega a resolver el problema se procede a reinstalar el aplicativo para tener un ambiente de producción totalmente nuevo, recuperando el aplicativo y las bases de datos que vinieran por defecto al momento de la instalación.
- e. Seguidamente se procede a solicitar un respaldo (archivo .wak), en este caso puede ser a uno de los niveles superiores de gestión de la información, ya sea a la Red, al SEDES, o finalmente podrán descargarlo de nuestro portal Web de consolidación.
- f. En caso de tener que hacer uso de los instrumentos manuales se procederá de la siguiente manera

En el plan de contingencias se debe tomar en cuenta el corte del sistema principal para realizar el registro de las atenciones en los establecimientos de salud que hace uso del SOAPS, ya que este puede ser por un tiempo indeterminado, por tal motivo se debe tener en cuenta que se deberá de realizar el registro de la información de manera manual (Registro de los instrumentos manuales establecidos por norma), como son los cuadernos del SNIS:

- a) Cuaderno 1 – Consulta Externa, enfermería y emergencias
- b) Cuaderno 2 – Atención Integral al Menor de 5 años
- c) Cuaderno 3 – Prenatal, parto, puerperio y planificación familiar
- d) Cuaderno 4 – Consultas y tratamientos Odontológicos
- e) Cuaderno 5 – Internaciones
- f) Cuaderno 6 – Actividades de Establecimiento y Comunidad

De la misma manera los formularios de consolidación:

- g) Form. 301a – Informe Mensual de Producción de Servicios 1er nivel.
- h) Form. 301b – Informe Mensual de Producción de Servicios 2do y 3er nivel.
- i) Form. 302ª – Notificación para Vigilancia epidemiológica

Este proceso hasta poder recuperar el sistema en su totalidad y continuar el proceso de manea digital.

En el plan de contingencias se debe tomar en cuenta el proceso de generación de las copias de seguridad del Sistema para evitar perdidas totales de las bases de datos que son utilizadas por el sistema SOASP.



Para tal efecto, en el establecimiento de salud, se programarán la generación de copias de seguridad periódicamente en coordinación con el personal del establecimiento que haga uso del sistema, para que así, se pueda tener un respaldo de las información que es introducida de manera diaria y en cada atención que es realizada.

Para el procedimiento de copia de seguridad se deben realizar las siguientes acciones:

- j) Realizar un respaldo de la base de datos (copia completa de las bases de datos del sistema .bak), periódicamente.
- k) Realizar un respaldo mediante el mismo sistema (copia mediante archivos .wak)
- l) Almacenado en medio físico, en custodia de un responsable del establecimiento.
- m) Documentación de las copias de seguridad.

Falla total o parcial de la red de comunicaciones: Si no se puede acceder al sistema SICE, debido a él no se tiene acceso a la red, se debe seguir los siguientes pasos:

1. El personal de sistemas o responsable de sistemas, debe verificar que los equipos de telecomunicaciones estén con energía, que estén distribuyendo señal correctamente.
2. Debe revisar que los cables de red estén conectados correctamente y armados según el estándar, de no ser así debe sacar el cable y volver a conectar.
3. Si el cable está funcionando incorrectamente, debe reemplazarlo.
4. Debe verificar que el hardware y/o del equipo para red este instalado correctamente.
5. De no lograr conectar el equipo a la red y el tiempo de espera sea mayor al tiempo de inactividad límite definido, se debe proceder a aplicar el proceso manual de registro de información, explicado en el proceso anterior.

n) Procedimientos de Recuperación

El plan de contingencias tecnológico es una estrategia que permite al personal de salud la solución y recuperación de información en un lapso de tiempo mediante procedimientos de contingencia.

- o) **Fase de Alerta.** Es la fase inicial en la cual se tiene conocimiento del incidente o evento, y se inicia la notificación para ejecutar el procedimiento correspondiente.
- p) **Fase de Contingencia.** Es donde se ejecutan todos los procedimientos de contingencia de acuerdo al recurso afectado.
- q) **Fase de Recuperación.** Es donde se vuelve a la normalidad con los recursos en funcionamiento normal y con todos los servicios en producción.

r) Medidas Preventivas

Como medidas preventivas a continuación se litan las estrategias del Plan:

Recurso Físico	Objetivo	Medida Preventiva
Equipo de computación	Asegurar el correcto funcionamiento de los equipos en los cuales se hace uso del Sistema SOAPS.	Soporte Técnico Preventivo
		Correcta instalación del software en equipos
		Mantenimiento Preventivo y correctivo de equipos de computación
red Informática	Asegurar el correcto enlace de	Correcto Cableado de red en ambientes del establecimiento



	equipos para un mejor rendimiento del sistema	Correcto armado de cables de red para evitar redundancia
		Correcta distribución de puntos de red de comunicación entre computadores.
Sistema de Información SOAPS	Asegurar correcto funcionamiento del aplicativo SOAPS	Correcta instalación del sistema SOAPS en los equipos de computación del establecimiento.
		Correcta actualización del sistema SOAPS.
información física y digital	Asegurar la información introducida en el SOAPS	Correcto llenado de la información en el sistema SOAPS
		Correcto generado de Copias de Seguridad del Sistema archivos .bak
		Correcto generador de archivos de respaldo archivos .wak

s) Recursos Necesarios para la recuperación

Recursos Necesarios	Descripción
Equipo de Computación o Servidor	Equipo de computación o servidor de características especiales para fungir el papel de servidor y poder alojar las bases de datos para el funcionamiento del Sistema SOAPS
Equipo de Computación o Cliente	Equipo de Computación para poder hacer uso del sistema en ambientes distintos al servidor y hace el registro de las atenciones en el sistema
Cableado Estructurado	Funcionamiento correcto del cableado estructurado sin cascadeo para poder tener una mejor transferencia de datos
Personal Capacitado	Personal con la capacidad y el conocimiento para poder realizar una restauración de una base de datos ya sea por medio de archivos wak o por copias de seguridad bak.
Copias de Seguridad disponibles	Copias de seguridad correctas, revisadas periódicamente verificando que no estén corruptas.

t) PLAN DE PRUEBAS

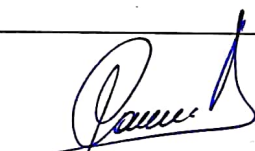
El plan de pruebas nos permitirá evaluar el desarrollo de las contingencias y reorientar o actualizar las acciones necesarias para superar los procesos críticos, el plan de pruebas que establecerá cada establecimiento de salud está en función de sus capacidades y tiempo definidos, el mismo debe contener mínimamente:



1. Riesgo y recurso a ser probado.
2. Responsables de la prueba: Ejecución y Evaluación.
3. Participantes de la Prueba.
4. Fecha y hora de inicio y conclusión.
5. Capacitación y entrenamiento previo.
6. Comunicación a los afectados con los servicios a ser suspendidos.
7. Las actividades propuestas en el plan deben ser probadas por lo menos una vez por año.
8. El Responsable de Seguridad Informática debe documentar las pruebas y los resultados.

Elaborado por: Herlan Cameo Ugarte
Fecha: 01/04/2019

Aprobado por: Rocco Abruzzese Castellón
Fecha: 01/04/2019


Ing. Herlan Cameo Ugarte
PROFESIONAL TÉCNICO II
SNIS - VE


Dr. Rocco Abruzzese Castellón
COORDINADOR NACIONAL SNIS - VE a.i
MINISTERIO DE SALUD
ESTADO PLURINACIONAL DE BOLIVIA