MINISTERIO de SALUD SNIS-VE	**PLAN DE CONTINGENCIAS** **UNIDAD:**SISTEMA NACIONAL DE INFORMACION EN SALUD Y VIGILANCIA EPIDEMIOLOGICA SNIS-VE **PROYECTO:** SOFTWARE SNIS	**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 del software del SNIS desarrollado por el Sistema Nacional de Información en Salud y Vigilancia Epidemiologica SNIS-VE, dependiente del Ministerio de Salud.

e) Definición de Procesos Críticos

- **Definición de eventos de Riesgo de TI**

Se realizo un análisis evento-causa para definir los riesgos más 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.

SISTEMA NACIONAL DE INF. EN SALUD Y VIGILANCIA EPIDEMIOLOGICA
V°B°
Rocco Coruzzese
COORD. SNIS-VE
M.S.

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) <u>Detalle de Procesos Críticos</u>

A continuación, se detallan los procesos críticos que interrumpirían el normal desarrollo del funcionamiento del software del SNIS:

- Falla total o parcial del equipo, el mismo que esta destinado para hacer uso del Software del SNIS, que puede ocurrir por algún factor personal o externo que afecta al funcionamiento del hardware y/o software base (programas propios del equipo de computación), aplicaciones de actualizaciones, factores externos, sobrecargas de corriente, falta de mantenimiento preventivo, fallas de fábrica, entre otras, que presente deficiencias que impiden el correcto funcionamiento del sistema o accesibilidad al mismo, si no se toma medidas inmediatas esto puedo ocasionar riesgos de perder parcial o totalmente la información.
- Falla de Actualización de Base de Datos y Aplicación del SNIS, el hecho de no manejar de forma sincronizada las últimas versiones de las aplicaciones, bases de datos y además de manera sincronizada, puede ocasionar que el usuario final tenga 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.

g) <u>Escenarios Previstos en Caso de Contingencias</u>

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

h) Falla total o parcial del equipo, el mismo que está destinado para hacer uso del Software del SNIS

- Se realiza el diagnóstico del problema en el Servidor (hardware/software), se quite al servidor de la red.
- Si es un problema de software o servicios del Servidor se procede a realizar el reinicio del servidor, verificando que todos los servicios se inicien correctamente.
- Si alguna de las bases de datos presenta problemas de inicio, se debe proceder a aplicar el procedimiento de recuperación de base de datos o puesta en modo de emergencia, esto les permitirá sacar una copia de seguridad o desacoplar la base para volverla a crear y posteriormente restaurar o adjuntar la base en observación.
- Si pese a este paso el gestor de base de datos no inicia o tiene deficiencias en su aplicación, se debe revisar los últimos programas instalados, proceder a desinstalarlos sin que afecten

VºBº Rocco Abruzzese COORD. NAL. SNIS-VE a.i. M.S.

a la base de datos, revisar las configuraciones del sistema, aplicar procesos de revisión de software malicioso, por medio u programa de antivirus.

- Desinstalar completamente el gestor de base de datos y volver a instalar, entendiendo que será necesario realizar el proceso de adjuntar los archivos copiados a la nueva instancia instalada.
- Solicitar un respaldo mediante las trasferencias correspondientes al nivel superior, pudiendo acudir hasta el nivel SEDES para tener un respaldo de la información que es enviada mensualmente mediante el sistema.

i) Falla de Actualización de Base de Datos y Aplicación del SNIS

- El responsable de sistemas o el área de sistemas de los niveles de gestión de la información, debe verificar que la versión se está aplica en el equipo de computación, estas versiones se publican de manera oficial en la página web del SNIS: https://snis.minsalud.gob.bo/snis
- Se debe aplicar las actualizaciones en los tiempos donde la actividad del sistema no sea crítica.
- En caso de que el tiempo de actualización del sistema 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.

En el plan de contingencias se debe tomar en cuenta el proceso de generación de las copias de seguridad del Sistema para evitar pérdidas totales de las bases de datos, generando una copia de las bases de datos por lo menos una vez al mes, específicamente la base de datos en la cual son almacenados los datos.

Para tal efecto, en el establecimiento de salud, se programarán la generación de copias de seguridad mensuales en coordinación con el personal del establecimiento que haga uso del sistema, para que así, se pueda tener un respaldo de la información que es introducida y realizar el conteo de las diferentes variables que están agrupadas en los formularios de consolidación.

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 la base de datos del sistema SNIS2019, según la gestión).
k) Almacenado en medio físico, en custodia de un responsable del establecimiento.
l) Documentación de las copias de seguridad con los datos necesario para tener un detalle de las copias realizadas por gestión.

En el plan de contingencias se debe tomar en cuenta el corte del sistema principal para realizar el registro de los datos consolidados que son generados a través de otros instrumentos en los establecimientos de salud que hace uso del Software del SNIS, 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:

Se deberá realizar el uso de los formularios de consolidación:

m) Form. 301a – Informe Mensual de Producción de Servicios 1er nivel.
n) Form. 301b – Informe Mensual de Producción de Servicios 2do y 3er nivel.
o) Form. 302a – Notificación para Vigilancia epidemiológica

SISTEMA NAC. DE INF. EN SALUD Y VIGILANCIA EPIDEMIOLÓGICA
Vº Bº
Rocco Abruzzese
COORD. NAC. SNIS-VE

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

p) 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 Software del SNIS.	Soporte Técnico Preventivo y correctivo
		Correcta instalación del software en equipos
		Mantenimiento Preventivo y correctivo de equipos de computación
Software del SNIS	Asegurar correcto funcionamiento del Software del SNIS	Correcta instalación del Software del SNIS en el equipo designado por el personal de salud.
		Correcta actualización del Software del SNIS en cuanto a aplicativo u estructura de establecimientos.
información física y digital	Asegurar la información introducida en el Software del SNIS	Correcto llenado de la información en el Software del SNIS siguiendo las reglas de validación introducidas en el software.
		Correcto generado de Copias de Seguridad del Software de la base de datos en la cual se almacena la información.
		Correcto generador de archivos de transferencias (archivos .ves) con la generación correspondiente del código hash de cada transferencia generada.

q) Recursos Necesarios para la recuperación

Recursos Necesarios	Descripción
Equipo de Computación	Equipo de Computación para poder hacer uso del sistema designado por el personal de salud.
Personal Capacitado	Personal con la capacidad y el conocimiento para poder realizar una recuperación de la información ya sea por base de datos o a través de las transferencias otorgadas por el nivel superior.
Copias de Seguridad disponibles	Copias de seguridad correctas y las transferencias, revisadas periódicamente verificando que no estén corruptas.

r) Plan de Comunicación y Activación de Contingencia

Si alguna de las contingencias se suscitase, se debe proceder de la siguiente manera para la comunicación y activación de la misma:

1. El usuario final reportará de la falta de acceso al sistema SNIS al encargado del sistema o personal de sistemas de manera inmediata, si fuera fin de semana lo hará por medios de comunicación existentes.
2. El encargado de sistemas o personal de sistemas realizara el diagnóstico de la interrupción y en función del proceso critico definirá el proceso de contingencia a aplicar, este proceso debe ser comunicado al director del hospital y parte administrativa y estadística de forma escrita y verbal según la criticidad, estos notificaran a los usuarios finales sobre el tema para que esperen los tiempos definidos, el tiempo que transcurrirá en aplicar las medidas de contingencia no debe superar el tiempo de inactividad mínimo definido, que permitan dar continuidad al servicio de información que el sistema provee.
3. Una vez que se haya aplicado la contingencia y restaurado los servicios se debe notificar al director, parte administrativa y estadística del restablecimiento de los servicios.

s) <u>Plan de Pruebas</u>

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 TECNICO II
SNIS - VE

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