N°23.....-2022-INSN-DG

RESOLUCION DIRECTORAL

Breña, 17 de Febrero de 2022

VISTO:

El Expediente con Registo N° 01123-2022, que contiene, Informe N° 028-2022-UI-OEI-INSN, Memorando N° 095-OEI-INSN-2022, Memorando N°126-OEPE-INSN-2022 y Memorando N° 151-2022-DG/INSN;

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 431-2015/MINSA, se aprueba el Documento Técnico: "Política de Seguridad de la Información del Ministerio de Salud", con la finalidad de mantener la continuidad de las operaciones del Ministerio de salud, en relación a los sistemas de información seguros, minimizando sus riesgos y maximizando los niveles de satisfacción de los usuarios;

Que, el artículo 20° del Reglamento de Organización y Funciones del Instituto Nacional de Salud del Niño, aprobado con Resolución Ministerial N° 083-2010-SA/DM, señala que la Oficina de Estadística e Informática, es el órgano encargado de conseguir que el Instituto cuente con un soporte informático, mecanización e integración de los sistemas de información requeridos para contribuir a la eficiencia de los procesos organizacionales;

Que, el Instituto Nacional de Salud del Niño, debe de contar con un plan de contingencias de plataforma de sistemas en el cual contenga procedimientos de información e instrucciones necesarias para responder eficazmente a una interrupción no deseada a las Bases de Datos alojadas en la Data Center donde residen los Sistemas Operativos y Administrativos de la Institución;

Que, en ese sentido se hace necesario aprobar el "Plan de Contingencias de Plataforma de Sistemas – OEI 2022" del Instituto Nacional de Salud del Niño con la finalidad de establecer procedimientos que debe aplicarse en todos los servicios de la Institución sobre el buen uso de los equipos de cómputo y lograr su óptimo funcionamiento;

Que, mediante Informe N° 126-OEPE-INSN, la Oficina Ejecutiva de Planeamiento Estratégico del Instituto Nacional de Salud del Niño emite opinión favorable a la propuesta del "Plan de Contingencias de Plataforma de Sistemas – OEI 2022";

Que, mediante documento de visto, el Director General del Instituto Nacional de Salud del Niño, remite el "Plan de Contingencias de Plataforma de Sistemas – OEI 2022" a la Oficina Ejecutiva de Planeamiento Estratégico el mismo que cuenta con la opinión favorabler de las instancias respectivas, para la elaboración de la resolución correspondiente;

Con el visado de la Oficina Ejecutiva de Planeamiento Estratégico, Oficina de Asesoría Jurídica y Oficina de Estadística e Informática del Instituto Nacional de Salud del Niño; y,

De conformidad con lo previsto en el Decreto Supremo N° 021-2017-SA y la Resolución Ministerial N° 083-2010/MINSA, que aprueba el Reglamento de Organización y Funciones del Instituto Nacional de Salud del Niño;

SE RESUELVE:

Artículo 1°. Aprobar el "Plan de Contingencias de Plataforma de Sistemas – OEI 2022" del Instituto Nacional de salud del Niño, el mismo que consta de diecisiete (17) folios y que forma parte de la presente resolución.

Artículo 2°. Encargar a la Oficina de Estadística e Informática la aplicación del mencionado Plan de Contingencias.

Artículo 3°. Encargar a la Oficina de Estadística e Informática la publicación de la presente Resolución en el Portal de Transparencia del Instituto Nacional de Salud del Niño.

Regístrese, comuníquese y publíquese.

MINISTERIO DE SALUD
INSTITUTO NACIONAL DE SALUD DEL NIÑO

M.C. JAIME AMADEO TASAYCO MUÑOZ
DIRECTOR GENERAL (e)
C.M.P. 18872 - R.N.E. 034554

JATM/NABN/JLSE/RACL.

DISTRIBUCION
( ) DG
( ) OEPE
( ) OAJ
( ) OEI
( ) Archivo

MINISTERIO DE SALUD
INSTITUTO NACIONAL DE SALUD DEL NIÑO
OFICINA DE ESTADISTICA E INFORMATICA
22 FEB. 2022
Folios: Firma: Hora: 8:44a
RECIBIDO

PLAN DE CONTINGENCIAS DE PLATAFORMA DE SISTEMAS – OEI

2022

Elaborado por: Ing. Christian Agreda **Cargo:** Seguridad Informática T.I **Fecha:** 20/01/2022	**Firma:**
Revisado por: Ing. Pedro López Berto **Cargo:** Especialista en Redes y Comunicaciones **Fecha:** 20/01/2022	**Firma:**
Aprobado por: Ing. Nicolas Bran Nizama **Cargo:** Jefe de la Oficina de Estadística e Informática **Fecha:** 20/01/2022	**Firma:**

CONTROL DE CAMBIOS				
ITEM	**TEXTO MODIFICADO**	**VERSION**	**FECHA**	**RESPONSABLE**
	Elaboración y Aprobación	1.0	20/01/2022	UNIDAD DE PLATAFORMA DE SISTEMAS

INDICE

1. OBJETIVO 5
2. ALCANCE 5
2.1. DEFINICION DE DESASTRE 6
2.2. ORGANIZACIÓN DEL PLAN 7
2.2.1. Escenarios Identificados como Posibles Contingencias: 8
2.3. Organigrama del Equipo de Rec. de los Sis. de In. base del INSN 9
3. Plan de Emergencia 9
3.1. Detección y Reacción – Notificación al Equipo de Seg. y Vig. del INSN. ...10
3.2. Declaración de Contingencia – Líder Técnico Administrador del Plan. 10
3.2.1. Equipo de Recuperación 11
3.3. Primeras acciones del Grupo Administrador del Plan 12
3.4. Operación temporal en el Local Sustituto 13
3.5. Restauración y retorno a un local permanente 13
4. Grupos y Responsabilidades 13
4.1. Grupo Administrador del Plan 14
4.2. Grupo de Sistemas de Información 17
4.3. Grupo de Plataforma 19
4.4. Grupo de Apoyo Empresa Proveedora 20
5. Administración de Backups de Contingencia 20
6. Mantenimiento y Pruebas del Plan 22
7. Administración de Registros Vitales 23
8. Anexo "A" 23
9. Anexo "B" 235
10. Anexo "C" 238
11. Anexo "D" 30
12. Anexo "E" 32
13. Anexo "F" 23

1. OBJETIVO

Establecer un procedimiento que debe aplicarse en todas las Unidades y Servicios del Instituto Nacional de Salud del Niño y ser administradas por la Oficina de Estadística e Informática sobre el Buen Uso de los Equipos de Cómputo, con el propósito de lograr su óptimo funcionamiento, continuidad en el servicio y la protección de la información procesada y almacenada en ellos.

2. ALCANCE

Este procedimiento contiene la información e instrucciones necesarias para que se pueda responder eficazmente a una interrupción no deseada a las Bases de Datos alojados en el Data Center donde residen los Sistemas Operativos y Administrativos del Instituto Nacional de Salud del Niño.

El alcance de esta contingencia es para las Bases de Datos siguientes con los siguientes niveles de prioridad (Anexo 01 – distribución de prioridades):

DBP01	-	Perteneciente a Economía
DBP02	-	Perteneciente a Sistemas_Asistenciales
DBP03	-	Perteneciente a Administrativo.
DBP04	-	Perteneciente a Sistemas_Complementarios.

Estos cuatro sistemas a partir de ahora los llamaremos “Sistemas de información Base del INSN”.

Las aplicaciones de estas cuatro bases de datos son en su mayoría aplicaciones CLIENTE-SERVIDOR por lo que toda la funcionalidad de las aplicaciones se encuentra en las Bases de Datos, de allí la importancia de tener disponibles estas Bases de Datos.

2.1. Definición de desastre

Para los términos de este procedimiento, desastre es el evento que sucede en el Data Center del INSN o en los equipos indispensables para su funcionamiento, que, por su característica o consecuencia, impide la normal actividad en éste durante un plazo estimado que NO es aceptable para los principales objetivos del servicio.

Se ha determinado que en estas cuatro Bases de Datos se encuentran los Sistemas Operativos y Administrativos del INSN, por lo que el mantener la operatividad de estos sistemas es primordial para el Instituto Nacional de Salud del Niño.

Se ha considerado un nivel de prioridad para la recuperación de estas Bases de Datos para de tal manera optimizar el uso de recursos disponibles durante la contingencia:

DBP01 - Prioridad 1, permitirá estabilizar la operación de los procesos de Economía

DBP02 - Prioridad 1, permitirá estabilizar la operación de los procesos de Sistemas_Asistenciales.

DBP03 - Prioridad 2, permitirá estabilizar la operación de los procesos Administrativos.

DBP04 - Prioridad 3, permitirá estabilizar la operación de los procesos de Sistemas_Complementarios.

Es así que este Plan tiene como misión permitir que en el evento de un desastre mayor en el Data Center donde residen estas bases de datos, se pueda seguir prestando los principales servicios como Sistema de Admisión, Egresos, Admisión de Emergencia, Sistema de Farmacia, Sistema de Seguro Integral de Salud (ambulatorio, hospitalizados), Sistema de Cuentas Corrientes, Sistema de Servicio Social, Sistema de Caja, Sistema de Consulta Externa, Sistema de Laboratorio, Sistema de Diagnóstico por Imágenes, así como la atención a nuestros clientes internos.

2.2. Organización del plan

El plan ha sido organizado de manera que los distintos grupos que conformen el Equipo de Recuperación tengan a su cargo los capítulos o secciones que se encuentren bajo su responsabilidad, de manera de facilitar las tareas de Mantenimiento y actualización del Administrador del Plan.

CAPITULO / ANEXO	RESPONSABLES
Cap. I. Objetivos	Grupo Administrador del Plan
Cap. 2. Plan de Emergencia	Grupo Administrador del Plan
Cap. 3. Equipos y Responsabilidades	Grupo Administrador del Plan
Cap. 4. Administración de Backups de Contingencia	Grupo Administrador del Plan/ Grupo de Sistemas de Información.
Cap. 5. Mantenimiento y Pruebas del Plan	Grupo Administrador del Plan/ Grupo de Sistemas de Información.
Anexo A Procedimiento de Contacto con Empresa Proveedora	Grupo Administrador del Plan/ Grupo de Sistemas de Información.
Anexo B Esquema de Operatividad de Alta Disponibilidad en los servidores de los Sistemas de información base del INSN (Cluster)	Grupo de Sistemas de Información.
Anexo C Detalle de Respaldos realizados en los Servidores de los Sistemas de información base del INSN	Grupo de Sistemas de Información.
Anexo D Esquemas de Recuperación de las bases de datos del Data Center.	Grupo de Sistemas de Información.
Anexo E Políticas de Seguridad de las bases de datos del Data Center	Grupo de Sistemas de Información.
Anexo F Red de Telecomunicaciones del Data Center	Grupo de Sistemas de Información.

2.2.1. Escenarios identificados como posibles contingencias:

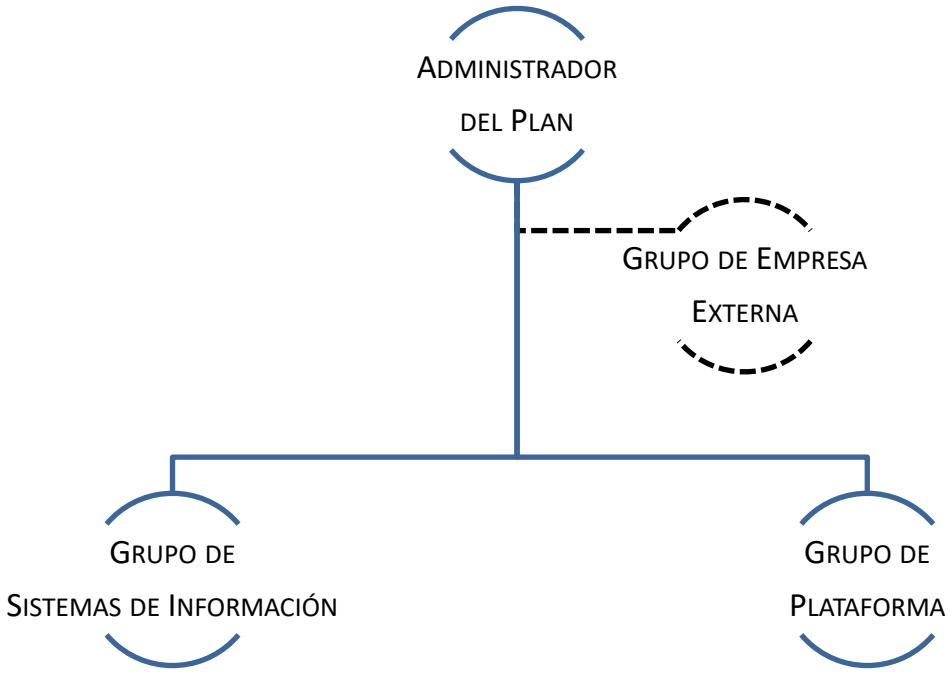
Los escenarios que se han identificado como posibles situaciones que ameriten la implementación de una acción de contingencia son los siguientes:

1.- Pérdida de Energía
A.- Corte Fluido General
B.- Corte Fluido Coordinado (con 2 horas de aviso)
C.- Corto Circuito
2.- Problema de Comunicación
A.- Interno
- Fibra Óptica
- Switch de la SAN
- Switch de comunicaciones
- Fallo del adaptador de red
B.- Externo
- Total
- Parcial
3.- Siniestro Total
A.- Desastre natural
B.- Incendio, inundación u otro daño
C.- Avería de los servidores (Disco duro, CPU, memoria, etc.)
4.- Otras Contingencias
- Fallo total de uno de los servidores
- Fallo de disco
- Fallo de fuente de poder de los servidores
- Fallo de equipos de telecomunicaciones (switch Core)
- Aparición de virus informáticos en los equipos
- Fallo del equipo de aire acondicionado
5.- Seguridad
- Control de password
- Control de Ingreso a sesión
- Control de acceso a las instalaciones del Data Center

2.3. Organigrama del equipo de recuperación de los sistemas de información base del INSN

El equipo de recuperación de los sistemas de información base del INSN estará conformado por los siguientes grupos:

- Administrador del Plan
- Grupo de Sistemas de Información
- Grupo de Plataforma
- Grupo de Empresa Soluzioni (Hasta Enero del 2021)



3. PLAN DE EMERGENCIA

En la presente parte del plan mencionaremos los procedimientos necesarios que deben ser realizados ante la ocurrencia de un evento que afecte el desarrollo normal de las operaciones del Data Center del INSN ubicado en el primer piso del edificio de OEAIDE.

El ciclo desde la ocurrencia de una interrupción hasta la total restauración del procesamiento normal tiene cinco fases:

- Detección y reacción.
- Declaración de Contingencia – líder técnico administrador del Plan.
- Primeras acciones del grupo administrador del plan.
- Operación temporal en el Local Sustituto.
- Restauración y retorno a un local permanente.

3.1. Detección y Reacción – notificación al equipo de seguridad y vigilancia del INSN

En cuanto suceda una situación de emergencia, en horario de oficina el personal de la Oficina de Estadística e Informática presente o el supervisor u el operador de turno del Data Center deberán contactar a las autoridades apropiadas, y luego seguir los pasos necesarios para minimizar el peligro o daño a las personas o a los activos del INSN.

3.2. Declaración de Contingencia – líder técnico administrador del Plan

Ante la presencia de un incidente el Líder Técnico del Grupo administrador del Plan es quien en primera instancia quien define si es necesario declarar el nivel de contingencia, lo cual debe ser ratificado por los demás miembros del Grupo administrador del Plan, para ello se debe realizar los siguientes pasos:

- Tan pronto como la interrupción ocurre el personal de la Oficina de Estadística e Informática presente o el supervisor u operador de turno del Data Center deberá notificar al líder técnico del Grupo Administrador del Plan explicándole el incidente.

- El líder técnico del Grupo Administrador del Plan es quien analizará el incidente y decidirá si declara el nivel de contingencia.

- El líder técnico del Grupo Administrador tiene la responsabilidad de contactar a los demás miembros del Grupo administrador del Plan a quien informará el incidente.

- Si la persona que detecta la emergencia no puede contactar al líder técnico del Grupo Administrador del Plan, entonces deberá notificar directamente a los demás integrantes del Grupo Administrador del Plan. Los miembros del grupo deben ser llamados en secuencia hasta que se localice a alguno de ellos.

- Dependiendo del escenario, el Grupo Administrador del Plan deberán contactar a los miembros de los otros grupos de Sistemas de Información, Plataforma y a la empresa Proveedora.

- Cuando un miembro de un grupo es localizado, esta persona se encargará de establecer contacto con los demás integrantes del grupo.

3.2.1. EQUIPO DE RECUPERACIÓN

La relación de los grupos de recuperación y sus líderes es la siguiente:

Grupo de Administración del Plan

NOMBRE	OFICINA	Celular	EMAIL
Nicolas Bran – Director de OEI	Anexo 1220	997717485	nbran@insn.gob.pe
Pedro Lopez – Encargado Unidad Informática	Anexo 1225	992794006	plopezb@insn.gob.pe
Christian Agreda – Seguridad Informática	Anexo 1225	960055990	cagreda@insn.gob.pe

Grupo de Sistemas de Información

NOMBRE	OFICINA	CELULAR	EMAIL
Martin Soberon Ramírez	Anexo 1224	981259343	msoberon@insn.gob.pe
Wilber Chuñocca Molina	Anexo 1224	990420992	wchunocca@insn.gob.pe
Rafael Arotinco Prado	Anexo 1224	991885748	rarotinco@insn.gob.pe
Víctor Antonio Lira Chumpitaz	Anexo 1224	993008350	vlira@insn.gob.pe

Grupo de Plataforma

NOMBRE	OFICINA	CELULAR	EMAIL
Pedro Lopez Berto	Anexo 1225	992794006	plopezb@insn.gob.pe
Nicolas Bran Nizama	Anexo 1225	997717485	nbran@insn.gob.pe
Cristian Agreda Romero	Anexo 1225	960055990	cagreda@insn.gob.pe
Ivan Garcilazo Ambukka	Anexo 1225	948549633	igarcilazo@insn.gob.pe
Christian Delgado Rivera	Anexo 1225	980483240	cdelgador@insn.gob.pe

Grupo de Apoyo Empresa Proveedora de Plataforma Central

NOMBRE	OFICINA	Celular	ACTIVO
ABRHAM PALOMARES	SOLUZIONI	983416708	FIREWALL INSN
LUIS PEREDA	SOLUZIONI	955020918	ANTISPAM

3.3. Primeras acciones del grupo administrador del plan

Coordinaciones iniciales

- Una vez que el Grupo Administrador del Plan, se ha declarado en nivel de Contingencia y que se ha comunicado a los miembros de los otros Grupos de Sistemas de Información, Plataforma y a la empresa Proveedora.

- En este momento se debe planear la reunión del grupo, bien sea en las propias instalaciones o cerca de ellas para hacer una primera evaluación de los daños. A continuación se determinará la acción a tomar y se notificará al grupo Administrador.

Establecimiento del Local Sustituto

Para el establecimiento de un local sustituto se debe tomar en cuenta:

- La primera tarea para el Grupo Administrador del Plan, es el establecimiento de un Data Center alterno.

- El Objeto del local sustituto es tener un área donde realizar las actividades de reactivación de los servicios del Data Center y además permitir una buena comunicación durante los períodos iniciales.

- Los teléfonos de contacto del Centro de Control se deberán suministrar a todas las áreas de la Oficina de Estadística e Informática y coordinadores de las principales áreas usuarias.

Inicio de Operaciones de los grupos de trabajo

Según sea el caso el Grupo Administrador del Plan determinará el Procedimiento a seguir dependiendo del nivel del desastre.

3.4. Operación temporal en el Local Sustituto

En los Capítulos y Anexos siguientes, se definen los Grupos y Procedimientos requeridos para el inicio de la operación temporal en el local sustituto. Para lograr un resultado exitoso de estos procedimientos, es necesario que el grupo administrador del plan mantenga un control periódico sobre:

- Disponibilidad de Recursos y Suministros.
- Ambiente de trabajo adecuado para cubrir las labores del proceso.
- Verificación de la Seguridad del local.
- Definición de los servidores alternos

3.5. Restauración y retorno a un local permanente

Una vez que los servidores alternos estén funcionando, se definirá un procedimiento para retornar al Data Center original. Una vez adecuado el local, se debe instalar el Hardware en forma permanente, e iniciar el proceso de retorno.

4. Grupos y Responsabilidades

Durante los procesos de desarrollo, realización de pruebas, e implementación del Plan, existen una serie de funciones y responsabilidades permanentes que recaen sobre los miembros que conforman el grupo de recuperación. La participación de los

grupos durante estos procesos permitirá tener un documento válido y grupos capaces de responder de acuerdo a los objetivos del Plan.

4.1. Grupo Administrador del Plan

El personal responsable de administrar el Plan es el siguiente:

NOMBRE	OFICINA	Celular	EMAIL
Pedro Lopez Berto	Anexo 1225	992794006	plopezb@insn.gob.pe
Nicolas Bran – Jefe de Unidad de Estadística e Informática	Anexo 1220	997717485	nbran@insn.gob.pe
Christian Agreda – Seguridad Informática	Anexo 1225	960055990	cagreda@insn.gob.pe

Las responsabilidades permanentes del Grupo Administrador del Plan son las siguientes:

Funciones del Grupo Administrador del Plan ANTES de un desastre.

El grupo administrador del plan deberá realizar las actividades necesarias como medidas de prevención antes de un desastre:

- Validar que el Plan obedezca los objetivos estratégicos del INSN, asegurando que permita la recuperación de las funciones críticas en los tiempos adecuados.
- Comunicar a los grupos que tendrán participación activa en la implementación del Plan.
- Revisar los reportes de proyectos, propuestas y procedimientos para los otros grupos.
- Difusión del Plan de Contingencia.
- Mantener la información actualizada.
- Realizar las pruebas del Plan.
- Asegurar que el local sustituto del servidor alterno esté lista para la gente y el grupo cuando sea necesario.

- Asegurar que las listas de requerimientos de los grupos de Desarrollo y de Telecomunicaciones estén disponibles inmediatamente después del desastre.
- Mantener un listado del equipo instalado en el INSN con sus características y números de serie. Esta información debe ser compartida con la compañía de seguro.

- Asegurar que se tenga la provisión para un mes, en un almacén fuera del local, de cualquier suministro de procesamiento de datos (cintas, cartuchos, etc.), que no se pueda obtener en menos de 24 horas.
- Asegurar que la información en custodia (cintoteca, etc.) esté respaldada en un almacén fuera del local, dentro de los tiempos especificados.
- Asegurar que toda la información para recuperación, almacenada lejos del Data Center está a salvo y pueda ser fácilmente recuperada por (y sólo por) las personas autorizadas.
- Planear, mantener, probar y auditar el sistema que mueve los registros vitales de todos los tipos al almacén fuera del establecimiento, y entonces recibirlos bajo condiciones controladas y mediante la autorización apropiada. Esto incluirá documentación en papel de este Plan de Recuperación, listas de los archivos requeridos y de cualquier impresión asociada, así como vaciados a cartuchos de Archivos, Base de Datos, Sistemas Operativos y Programas de Aplicación.
- Definir los equipos a utilizarse como servidor alterno.
- Definir la ubicación del local sustituto donde funcionaran los servidores alternos.

Funciones del Grupo Administrador del Plan DURANTE el desastre.

- Declarar que el Plan de Recuperación será puesto en ejecución.
- Instruir al líder del Grupo de Sistemas de Información para que recupere los documentos vitales para contingencia (manuales y procedimientos) que se encuentren resguardados en lugar seguro.
- Determinar la disponibilidad de todos los empleados del equipo de Recuperación.

- Decidir la convocatoria de los líderes de grupo y miembros alternos en caso necesario.
- Poner una copia de todo el material en el local sustituto.
- Decidir sobre la ubicación del servidor alterno y asegurar su disponibilidad.
- Administrar el Plan de Recuperación desde el local sustituto.
- Dar guía a los otros grupos (Sistemas de Información y Plataforma).
- Arreglos para realizar los gastos y pago de facturas.

- Mantener informada a la Dirección de la Oficina de Estadística e Informática.
- Dar las directivas para realizar los principales procesos operativos mientras se recuperan los “Sistemas de información base del INSN”
- Adecuar el local sustituto con la lista de los equipos y materiales a utilizar.
- Proveer al personal de facilidades de transporte.
- Comunicar números de teléfono y ubicación del local sustituto a todos los miembros de los grupos, y a las áreas clientes o que están involucradas en el sistema.
- Preparar las facilidades de restauración para recibir equipo eléctrico, teléfonos, etc.
- Supervisar la instalación física del equipo, líneas telefónicas, mobiliario, y de todo lo necesario para el ambiente de trabajo de los grupos de recuperación.
- Arreglar cualquier asistencia necesaria en la localidad de restauración al Grupo de Sistemas de Información.
- Ordenar los reemplazos de acuerdo a requerimientos actualizados. Ser cuidadosos en la selección del nuevo equipo. Se puede solicitar equipo más actualizado tecnológicamente con mejores o iguales precios; pero se debe tener cuidado con cambios innecesarios de versiones.
- Tener los listados, cartuchos, discos y diskettes, de los cuales el grupo es responsable, recuperados del almacén dentro de los tiempos establecidos.
- Hacer copias suficientes de este Plan de Recuperación, para todos los líderes de los grupos de Sistemas de Información y Plataforma.

4.2. Grupo de Sistemas de Información

NOMBRE	OFICINA	CELULAR	EMAIL
Martin Soberon Ramírez	Anexo 1224	981259343	msoberon@insn.gob.pe
Wilber Chuñocca Molina	Anexo 1224	990420992	wchunocca@insn.gob.pe
Rafael Arotinco Prado	Anexo 1224	991885748	rarotinco@insn.gob.pe
Víctor Antonio Lira Chumpitaz	Anexo 1224	993008350	vlira@insn.gob.pe

Las responsabilidades permanentes del Grupo de sistemas de información del Plan son las siguientes:

Funciones del Grupo de Sistemas de Información ANTES de un desastre.

- Apoyar al grupo administrador del Plan para que los planes para el respaldo y restauración de cualquier aplicación vital estén completos, reflejen los cambios como ocurren y sean validados para su confiabilidad dos veces al año, mediante la prueba correspondiente.
- Trabajar con el Grupo Administrador del Plan para asegurarse que las distintas formas de respaldo estén a salvo y organizadas para una rápida recuperación.

Funciones del Grupo de Sistemas de Información DURANTE el desastre.

- Recuperar la documentación necesaria prevista.
- Recuperar todo el material de respaldo incluyendo la documentación listada en los procedimientos de respaldo de la aplicación.
- Trabajar con los otros grupos en la implementación del local sustituto asignado para la recuperación del sistema.
- Hacer inmediatamente un backup del Sistema y de los registros vitales, llevándolos fuera de la localidad.

- Ejecutar y/o coordinar con los proveedores de apoyo los trabajos de recuperación; como restaurar cartuchos, instalación del sistema operativo
- Creación de base de datos, realizar actividades de export/import, instalación de softwares y otras actividades para la restauración del servicio.

- Cuando el sistema restaurado esté disponible, iniciar la “ejecución” de aplicaciones en la secuencia previamente especificada.
- Mantener al Grupo Administrador del Plan informado de su actividad.

- Asegurar el funcionamiento de los programas del sistema que sean necesarios para el servidor alterno.
- Tener los programas, drivers y cualquier documentación y procedimiento asociados, en los paquetes estándar del sistema. Esto asegurará su disponibilidad cuando sea necesario.
- Establecer los requerimientos del Sistema Operativo de archivos, bibliotecas y utilitarios del sistema.
- Asegurar que los cambios anteriores a los programas del sistema sean completos, reflejen los cambios cuando ocurran y sean validados con exactitud en los tiempos apropiados.
- Asegurar que todos los programas pueden correr en equipo de reemplazo.
- Ordenar cualquier elemento necesario de las listas de las cuales el grupo es responsable.
- Cargar y probar el sistema operativo y otros sistemas y archivos.
- Coordinar con los grupos administrador del plan y el de Plataforma.
- Asegurar que cada aplicación sea restaurada sin pérdida de Registros Vitales.
- Poner en funcionamiento del servidor alterno de los sistemas de información base del INSN.

4.3. Grupo de Plataforma

NOMBRE	OFICINA	CELULAR	EMAIL
Pedro Lopez Berto	Anexo 1225	992794006	plopezb@insn.gob.pe
Nicolas Bran Nizama	Anexo 1220	997717485	nbran@insn.gob.pe
Cristian Agreda Romero	Anexo 1225	960055990	cagreda@insn.gob.pe
Ivan Garcilazo Ambukka	Anexo 1225	948549633	igarcilazo@insn.gob.pe
Luis Cardenas Abarca	Anexo 1225	980483240	lcardenas@insn.gob.pe

Las responsabilidades permanentes del Grupo de Plataforma son las siguientes:

- Asegurar que el grupo de Plataforma y las líneas estén disponibles (en los casos en que éstas estuviesen previstas para el Procedimiento).
- Planear y probar la capacidad de establecer comunicación remota desde el local alterno.
- Mantener copias de los sistemas, configuraciones y drivers de los equipos de telecomunicaciones (Routers, Pads, switch, entre otros.) así como los procedimientos de su configuración.
- Apoyar al grupo administrador del Plan para que los planes para el respaldo y restauración de cualquier aplicación vital estén completos, reflejen los cambios como ocurren y sean validados para su confiabilidad dos veces al año, mediante la prueba correspondiente.
- Trabajar con el Grupo Administrador del Plan para asegurarse que las distintas formas de respaldo estén a salvo y organizadas para una rápida recuperación.

Funciones del Grupo de Soporte de Telecomunicaciones DURANTE el desastre.

- Verificar la operación de la red alterna una vez se tenga el sistema restaurado.
- Ordenar líneas, terminales y módems si se requiere.
- Probar las líneas directas y de comunicación al servidor de bases de datos del INSN donde residen los Sistemas Operativos y Administrativos del INSN.

- Restaurar y probar las comunicaciones hacia los servidores bases de datos del INSN donde residen los Sistemas Operativos y Administrativos del INSN.
- Asistir al grupo de mantenimiento para monitorear y controlar la red.
- Mantener al Grupo Administrador del Plan informado de su actividad.

4.4. Grupo de Apoyo Empresa Proveedora

- Dado que los equipos con los que se cuenta son equipos de seguridad perimetral que se encuentran dentro de los tres (03) años de garantía y soporte (Desde el 15/05/2019 hasta el 15/05/2022) brindado por SOLUZIONI (Compañía que brinda el servicio de seguridad perimetral al INSN incluyendo el servicio de soporte y mantenimiento), el primer paso que habría que considerar es contactar al supervisor del servicio por parte de SOLUZIONI para que preste el apoyo necesario en la etapa de recuperación del sistema ya sea como pare del servicio en caso que aplique y/o con servicios adicionales.

NOMBRE	OFICINA	Celular	EMAIL
ABRHAM PALOMARES - Líder Técnico	E. externa	983416708	apalomares@soluzioniinternational.com

5. ADMINISTRACIÓN DE BACKUPS DE CONTINGENCIA

El respaldo de los servidores de bases de datos del INSN, puede ser manejado en tres categorías:

- Backup de software base (sistema operativo y productos utilitarios)
- Backup de aplicaciones
- Backup de datos

- Cada una de estas categorías tiene un manejo con características propias.
- El Backup de software base es en prevención de que los originales por manipulación o deterioro no puedan ser instalados en el momento de la contingencia.
- El backup de aplicaciones y de datos debe ser realizado con mayor continuidad, debido a las características de desarrollo y mantenimiento permanente de los de los Sistemas de información base del INSN y debido al control que se tiene de esta información, es factible manejar la frecuencia de actualización de estos backups de un modo dinámico.

Para cubrir estas tres categorías es necesario mantener un plan de rotación de los backups, el procedimiento a seguir para este intercambio seria el siguiente:

- Se debe realizar dos copias de backup diarias las cuales formarán parte del juego de backup de almacenamiento en el local del Data Center.
- Se debe enviar una copia de los backups cada dos (02) días hacia la empresa que presta el servicio de almacenamiento de los tapes en un local externo (solo si la entidad cuenta con este servicio con alguna empresa de seguridad).
- Se debe considerar que cuando haya alguna modificación en aplicaciones o software base, seguida de uno o más días sin modificación, se deben tomar las medidas para mantener el último nivel de actualización en todas las versiones backup.

La distribución de las copias será la siguiente:

- Diariamente se ejecutará backups que serán almacenados localmente en el Data Center del INSN.
- En forma interdiaria se enviará una copia de los backups a la empresa externa encargada del respaldo de los tapes.
- Los días restantes el juego de backup se quedará en el Data Center del INSN.

6. MANTENIMIENTO Y PRUEBAS DEL PLAN

Para el mantenimiento del Plan de Contingencia, es necesario desarrollar un conjunto de pruebas en el local sustituto. Estas pruebas deben asegurar el buen funcionamiento de todas las actividades que sería necesario realizar en caso que se presenten las situaciones de emergencia que impliquen el uso de este servicio.

Las actividades que normalmente deben ser contempladas en estas pruebas son:

- Contacto con las personas involucradas en los grupos de apoyo de contingencia.
- Contacto con las personas responsables del local y servidores alternos.
- Contacto con La Unidad de Sistemas de Información.
- Revisión del material de contingencia: Procedimientos, Cartuchos, Backup y Suministros.
- Ejecución de los procedimientos de recuperación del sistema operativo y base de datos en el servidor alterno.
- Carga de los archivos actualizados en el servidor alterno de respaldo.
- Revisión de la funcionalidad de los “Sistemas de información base del INSN” instalados en el servidor alterno.
- Revisión de la información resultante de las pruebas.
- Las cuatro primeras actividades deben ser realizadas periódicamente para efectos de comprobación y mantenimiento.

7. ADMINISTRACIÓN DE REGISTROS VITALES

Los registros vitales son el conjunto de documentos necesarios, como planes y procedimientos para poder realizar una correcta recuperación de los Sistemas de información base del INSN.

Para la administración de los registros vitales de los “Sistemas de información base del INSN” se deberá tener un juego impreso en los locales de respaldo:

- Cintoteca del INSN ubicada en el local de la Av. Brasil 600 – Breña
- Domicilio del personal del Grupo Administrador del Plan

La lista de los documentos que forman parte de los registros vitales está descrita en el anexo H del presente documento.

ANEXO A

- Contacto con Empresa Proveedora
- La persona de contacto por parte del proveedor a quien los miembros del Grupo Administrador del Plan deben llamar es al Líder técnico del proveedor.
- Es esa persona la que dispondrá de la disponibilidad de los recursos de personal y hardware si es necesario.

Los datos de las personas de contacto de la empresa IBM del Perú son:

NOMBRE	OFICINA	Celular	EMAIL
ABRHAM PALOMARES - Líder Técnico	E. externa	983416708	apalomares@soluzioniinternational.com

ANEXO B

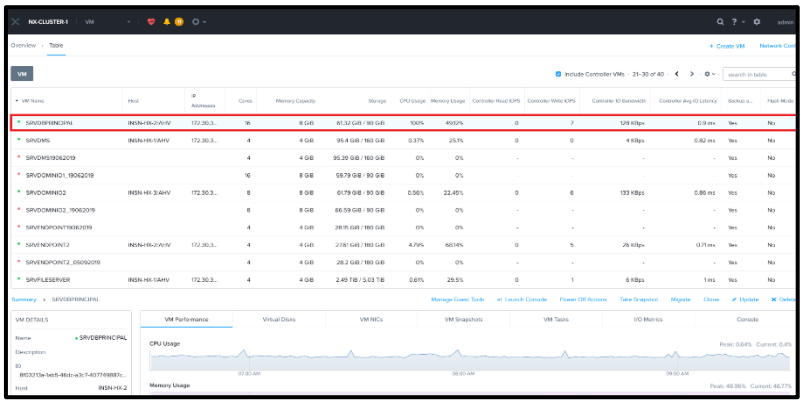
Características de análisis y administración

La solución a proveer deberá permitir:

- Analizar en forma grafica el impacto que tiene un evento con el comportamiento de la plataforma global y/o con el comportamiento de una maquina virtual, a nivel de CPU, memoria y disco.
- Determinar en tiempo real el consumo de los recursos de CPU, memoria ram y disco.
- Entregar estadísticas completas sobre la maquinas virtuales, como consumos de vCPU, ram y discos, y de IOPS de lectura, IOPS de escritura y latencias.
- Entregar un análisis detallado de donde se están sirviendo los IOPS, ya sea de discos SSD, HDD.
- Analizar el ancho de banda utilizado por la misma, así como el ancho de banda utilizado por una máquina virtual.

La consola de administración deberá:

- Ser accedida mediante un browser y estar basada en HTML5.
- Proveer una única vista para todo el entorno manteniendo múltiples puntos de acceso.
- La consola de administración deberá permitir administrar y monitorear a todos los servidores/nodos que forman parte del Cluster, así como el hipervisor y toda la plataforma virtual.



Falla de un servidor del Clúster de Base de Datos.

La configuración escogida para la alta disponibilidad que permite que ambos componentes del clúster mantengan su carga respectiva y adicionalmente el servidor de alterno soporte automáticamente la carga del servidor principal del Clúster en caso de inoperatividad del mismo y viceversa.

Una vez de reparada la falla que el servidor que sufrió este podrá readquirir sus recursos en forma programada.

Falla Del Adaptador De Red.

En el caso de falla de un adaptador de red cada uno de los servidores tiene habilitado el 2 tarjetas de FC habilitados en tranking y 2 tarjetas de UTP habilitadas también en tranking, esto permitirá que si falla una de las tarjetas de red de FC la otra tarjeta de FC seguirá trabajando sin ocasionar problemas de pérdidas de comunicación, lo mismo sucedería ante la pérdida de una tarjeta UTP.

Falla De Disco.

Ante la falla de un disco, el servidor de almacenamiento está configurado en un arreglo RAID 1 y RAID5, lo cual evitará la perdida de datos del sistema, adicionalmente el servidor de almacenamiento cuenta con discos SPARE que reemplazarán automáticamente al disco averiado, esta protección es automática y no afecta al usuario final, paralelamente el equipo envía una alerta al proveedor quien coordina con el personal de la Unidad de Plataforma de Sistemas de la Oficina de Estadística e Informática del INSN el reemplazo del disco averiado.

Falla de Fuente de Poder de los Servidores.

Ante la falla de una fuente de poder cada servidor IBM cuenta con módulos de hardware en redundancia para fuente de poder y ventiladores internos, asegurando de esta manera la continuidad de operación de los servidores en caso de falla de una fuente de poder.

Falla de Equipos de Telecomunicaciones.

Ante la falla de uno de los switch de la red LAN del Data Center se cuenta con un switch en redundancia el cual asumiría toda la carga del equipo averiado, asegurando de esta manera la continuidad de operación de los servicios en caso de falla de un switch de la red LAN del Data Center.

ANEXO C

Detalle de Respaldos realizados en los Servidores de las de las Bases de datos de Plataforma Central

Los respaldos se han dividido en tres tipos:

- Respaldo de los softwares de instalación del sistema (Sistema Operativo, Software IBM, Base de datos SQL,etc).
- Respaldo de las aplicaciones (Programas Fuentes, Archivos de Salidas, Archivos de Configuración)
- Respaldo de la base de datos.

En el siguiente documento se indican los recursos necesarios para llevar a cabo, correctamente, el procedimiento de ejecución de copias de respaldo y rotación de cartuchos. Además hacemos entrega del procedimiento para llevar a cabo estos respaldos, necesarios para evitar cualquier problema de pérdida de información.

1. Nombrar las personas responsables de la ejecución de los procedimientos de respaldo.
2. Determinar los recursos necesarios para llevar a cabo los procedimientos de respaldo.
3. Evitar cualquier tipo de perdida de información que podría involucrar críticamente la restauración de los Sistemas de información base del INSN.

RESPONSABILIDAD Y RECURSOS

Responsables:

NOMBRE	OFICINA	CELULAR	EMAIL
Martin Soberon Ramírez	Anexo 1224	981259343	msoberon@insn.gob.pe
Wilber Chuñocca Molina	Anexo 1224	990420992	wchunocca@insn.gob.pe
Rafael Arotinco Prado	Anexo 1224	991885748	rarotinco@insn.gob.pe
Víctor Antonio Lira Chumpitaz	Anexo 1224	993008350	vlira@insn.gob.pe

Recursos:

Respaldo de los softwares de instalación:

- ✓ Los softwares a respaldar son:
- ✓ Sistema Operativo Windows 2012 Server
- ✓ Software Alta disponibilidad IBM
- ✓ Otro Software
- ✓ Microsoft SQL Server 2012
- ✓ Microsoft SQL Server 2008
- ✓ Otro Software
- ✓ Parche de base de datos SQL

Se debe contar con una copia de los cd's en la Oficina de Estadística e Informática del INSN y un juego de los cd's en el ambiente del site de contingencia.

Respaldo de las aplicaciones y de base de datos:

El detalle del respaldo de las aplicaciones y de la base de datos se elabora por parte del personal de plataforma en conjunto con el personal de desarrollo.

ANEXO D

Esquemas de Recuperación de las bases de datos del INSN.

1.- Pérdida de Energía Eléctrica

CAUSAS	CONSECUENCIAS	ACCION A TOMAR
A.- Corte no planificado del Fluido Eléctrico General	Pérdida de Servicio general	El operador de turno del Data Center deberá: - Avisar y coordinar con el personal de la Unidad de Plataforma de Sistemas de turno, quienes indicaran la duración de incidente. - Avisar y coordinar con el personal de la Unidad de Plataforma de Sistemas, informando los servicios afectados. - Cuando el personal de la Unidad de Plataforma de Sistema indique que se restableció y estabilizó el fluido eléctrico se deberá comunicar a la Oficina de Estadística e Informática quien indicará el inicio del restablecimiento de los servicios.
B.- Corte Planificado del Fluido Eléctrico (con 2 horas de aviso como mínimo)	Pérdida de Servicio general	El operador de turno deberá apagar el equipamiento del centro de cómputo, previa autorización del personal de soporte técnico, para ello deberá reunirse con los equipos y evaluar el impacto: Cuando el personal de la Unidad de Plataforma de Sistemas indique que se restableció y estabilizo el fluido eléctrico se deberá comunicar a la Oficina de Estadística e Informática quien indicara el inicio del restablecimiento de los servicios.

2.- Problema de Comunicación

CAUSAS	CONSECUENCIAS	ACCION A TOMAR
A.- Interno - Switch Principal. - Router Principal - Fibra Optica.	-Pérdida de Servicio Total	- Avisar y coordinar con el personal de la Unidad de Plataforma de Sistemas. - Si el problema se presenta en la infraestructura de las telecomunicaciones el encargado de reestablecer el servicio seria el equipo de Plataforma. -. Ejecutar cambios de equipos con el proveedor o ver en stock si contamos con equipos de repuestos.

3.- Siniestro Total

CAUSAS	CONSECUENCIAS	ACCION A TOMAR
A.- Desastre natural, Incendio, inundación u otro daño	-Pérdida total de Data Center	- Ejecución del Plan de emergencia. - Verificar la operatividad de los equipos del Data Center. - Evaluar daños - Dimensionar tiempo de recuperación - Tomar medidas necesarias - Habilitar servicios - Verificar disponibilidad de cartuchos - Restore de información - Puesta en servicio del sistema. - Habilitar el servidor alterno, las características y servicios mínimos la lista de servicios por servidor.

ANEXO E

Políticas de Seguridad de las bases de datos del Data Center del INSN

Como parte de la política de seguridad de la plataforma se ha implementado:

I. Niveles de Acceso.
II. Sistema contra incendios.
III. Sistema de aire acondicionado.
IV. Sistema de detección de inundación.

I. NIVELES DE ACCESO

Los niveles de acceso se han dividido en 2 capas

- Nivel Lógico
- Nivel Físico

Nivel de Acceso Lógico:

Identificación por Huella Dactilar para obtener acceso al Data Center, con registros de acceso.

- Privilegios de cada Usuario
- Actualmente cada usuario tiene asignado un Perfil de Usuario a nivel de aplicación el cual le dará ciertos privilegios de acceso, consultas y modificaciones al sistema de Control de Acceso.
- La modificación de los perfiles de usuario es solicitada a la Unidad de Plataforma de Sistemas de la Oficina de Estadística e Informática.

Nivel de Acceso Físico:

Se ha implementado las siguientes medidas para Control de acceso a las instalaciones del Data Center donde se encuentran ubicados los servidores de los Sistemas de información base del INSN.

En las instalaciones del Data Center de los Sistemas de información base del INSN el ingreso es restringido teniendo una única puerta de acceso a las instalaciones, esta se encuentra permanentemente cerrada y solo

II. SISTEMA CONTRA INCENDIOS

Hay un proyecto de un sistema contra incendio el cual utiliza el gas **FM2000** que actúa como agente extintor del fuego, no afecta a los medios electrónicos y tampoco a los seres humanos, este agente se encuentra almacenado en el balón instalado en el Data Center.

SISTEMA DE AIRE ACONDICIONADO.

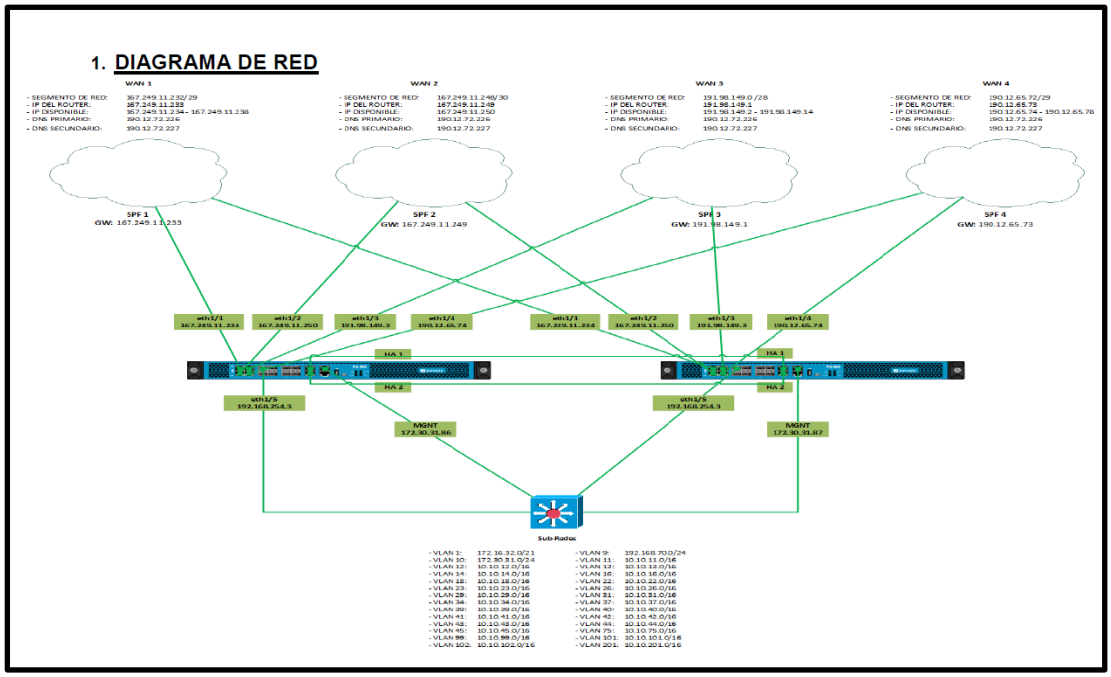
Se tiene implementado en el Data Center un sistema de aire acondicionado de Alta Precisión que mantiene la temperatura y la humedad del ambiente del Data Center en el rango adecuado para la operación de los servidores del INSN.

SISTEMA DE DETECCION DE INUNDACION Y CONTROL DE TEMPERATURA.

Se tiene implementado en el Data Center un sistema de detección de inundación y control de la temperatura en las instalaciones del Data Center, este sistema envía correos si se presentase algún incidente de inundación o variación de temperatura fuera de los límites normales, además cuenta con una pantalla de monitoreo que muestra el estado de las variables que se monitorea.

La ruta de acceso es: http://x.x.x.x/login

ANEXO F

Red de Telecomunicaciones del INSN

El siguiente diagrama representa un esquema de la distribución de la red LAN la cual es administrada por el equipo de plataforma del INSN.