REPÚBLICA DEL PERÚ

Resolución de Dirección Ejecutiva

N° 344 -2018-MIDIS/PNAEQW

Lima,

VISTOS: 18 SET. 2018

El Memorando N° 376-2018-MIDIS/PNAEQW-UTI, de la Unidad de Tecnologías de la Información; el Memorando N° 3029-2018-MIDIS/PNAEQW-UPPM, de la Unidad de Planeamiento, Presupuesto y Modernización; y, el Informe N° 811-2018-MIDIS/PNAEQW-UAJ, de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 008-2012-MIDIS, y sus modificatorias, se crea el Programa Nacional de Alimentación Escolar Qali Warma (en adelante, PNAEQW), como Programa Social del Ministerio de Desarrollo e Inclusión Social (en adelante, el MIDIS), con la finalidad de brindar un servicio alimentario a los escolares de las instituciones educativas públicas bajo su cobertura;

Que, los literales e) y g) del artículo 25 del Manual de Operaciones del PNAEQW, aprobado por Resolución Ministerial N° 283-2017-MIDIS, establece que la Unidad de Tecnologías de la Información tiene, entre otras funciones: *e) Proponer y/o actualizar documentos normativos orientados a la gestión, planeamiento, desarrollo y seguridad de las tecnologías de información y comunicaciones del Programa, en el marco de lo dispuesto por el MIDIS y PCM (...); y, g) Definir e implementar mecanismos de seguridad y mantenimiento óptimo de los sistemas de información que contienen las bases de datos requeridas para las actividades administrativas y operativas del Programa*;

Que, mediante Resolución de Dirección Ejecutiva N° 9789-2015-MIDIS/PNAEQW, se aprueba la "Directiva para la Formulación, Revisión y Aprobación de los Documentos Normativos en el PNAEQW", mediante la cual se establecen disposiciones para la formulación, revisión, y aprobación de los documentos normativos que requieren los procesos que llevan a cabo las Unidades orgánicas del PNAEQW;

Que, mediante Memorando N° 376-2018-MIDIS/PNAEQW-UTI, la Unidad de Tecnologías de la Información presenta el proyecto de Plan de Contingencia de Tecnologías de la Información del PNAEQW, el cual tiene como objetivo garantizar la continuidad de los servicios de tecnologías de la información de la Sede Central;

Que, mediante Memorando N° 3029-2018-MIDIS/PNAEQW-UPPM, la Unidad de Planeamiento, Presupuesto y Modernización señala que no se cuenta con otro documento que colisione o se superponga con el plan materia de análisis; asimismo que dicho proyecto no irroga gastos presupuestales adicionales a los aprobados como parte de las actividades del Plan Operativo Institucional – POI; y, que cumple con la "Directiva para la Formulación, Revisión y Aprobación de los Documentos Normativos en el PNAEQW"; por lo que opina favorablemente por la aprobación del mencionado proyecto de documento normativo;

Que, mediante el informe del visto, la Unidad de Asesoría Jurídica opina que el proyecto de plan presentado por la Unidad de Tecnologías de la Información y revisado por la Unidad de Planeamiento, Presupuesto y Modernización, cumple con las condiciones señaladas en la "Directiva para la Formulación,

Revisión y Aprobación de los Documentos Normativos en el PNAEQW", aprobado por Resolución de Dirección Ejecutiva N° 9789-2015-MIDIS/PNAEQW;

Con el visado de la Unidad de Tecnologías de la Información, la Unidad de Planeamiento, Presupuesto y Modernización; y, la Unidad de Asesoría Jurídica;

En uso de las atribuciones establecidas en el Decreto Supremo N° 008-2012-MIDIS, Decreto Supremo N° 006-2014-MIDIS, Decreto Supremo N° 004-2015-MIDIS, Decreto Supremo N° 012-2017-MIDIS, Decreto Supremo N° 005-2018-MIDIS, la Resolución Ministerial N° 283-2017-MIDIS, y la Resolución Ministerial N° 232-2018-MIDIS;

SE RESUELVE:

Artículo 1. Aprobación del Plan de Contingencia de Tecnologías de la Información del Programa Nacional de Alimentación Escolar Qali Warma

Aprobar el "Plan de Contingencia de Tecnologías de la Información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo PLA-015-PNAEQW-UTI, que forma parte integrante de la presente resolución.

Artículo 2. Comunicación a las Unidades Territoriales, Unidades de Asesoramiento, Apoyo y Técnicas del Programa Nacional de Alimentación Escolar Qali Warma

Encargar a la Coordinación de Gestión Documentaria y Atención al Ciudadano, hacer de conocimiento de la presente Resolución a las Unidades Territoriales, las Unidades de Asesoramiento, Apoyo, y Técnicas del Programa Nacional de Alimentación Escolar Qali Warma, a través de medios electrónicos.

Artículo 3. Publicación en el Portal Institucional

Publicar la presente Resolución de Dirección Ejecutiva, en el Portal Institucional del Programa Nacional de Alimentación Escolar Qali Warma (www.qaliwarma.gob.pe).

Regístrese y comuníquese.

SANDRA NORMA CÁRDENAS RODRÍGUEZ
Directora Ejecutiva
Programa Nacional de Alimentación Escolar Qali Warma
Ministerio de Desarrollo e Inclusión Social

QaliWarma
PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR

PERÚ | Ministerio de Desarrollo e Inclusión Social | Viceministerio de Prestaciones Sociales | Programa Nacional de Alimentación Escolar QALI WARMA

PLAN

Código de documento normativo	Versión N°	Total de Páginas	Resolución de aprobación	Uso Interno Aprobación
PLA- -PNAEQW-UTI	01	26	Resolución de Dirección Ejecutiva N° -2018-MIDIS-PNAEQW	/ /

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA

ELABORADO POR:	REVISADO POR:	REVISADO POR:
Jefa de la Unidad de Tecnologías de la Información Firma	Jefa de la Unidad de Planeamiento, Presupuesto y Modernización Firma	Jefe de la Unidad de Asesoría Jurídica Firma
SOLEDAD ADELA GANOZA ESPEJO Jefa de la Unidad de Tecnologías de la Información Programa Nacional de Alimentación Escolar Qali Warma Ministerio de Desarrollo e Inclusión Social	JENNY REINO SÁENZ Jefa de la Unidad de Planeamiento, Presupuesto y Modernización PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL	BORIS GONZALO POTOZÉN BRACO Jefe de la Unidad de Asesoría Jurídica PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL
Fecha elaboración:	Fecha de Revisión:	Fecha de Revisión:

ÍNDICE

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA
VºBº
JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN
MIDIS

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA
V° B°
B. MORALES C.

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL PROGRAMA NACIONAL DE ALIMENTACION ESCOLAR QALI WARMA

I. PRESENTACIÓN

1.1. El Plan de Contingencia de Tecnologías de la Información del Programa Nacional de Alimentación Escolar Qali Warma, (PNAEQW), es un documento que establece los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, las interrupciones ocasionadas a los servicios críticos de Tecnologías de la Información (TI), producto de desastres, eventos naturales o producidos por el hombre. Los servicios críticos de TI se encuentran alojados en los servidores del Centro de Datos ubicados en la Unidad de Tecnologías de la Información.

1.2. El presente documento sirve como marco de referencia para la elaboración de las políticas, normas y procedimientos de contingencias respecto a las Tecnologías de la Información. Por consiguiente, se han definido las acciones que se deben seguir en el momento de presentarse una contingencia que afecte los servicios para mantener o reestablecer el servicio en el menor tiempo posible, acciones que se encuentran definidas teniendo en cuenta la disponibilidad de recursos físicos y humanos en el presente documento.

1.3. La elaboración del Plan de Contingencia implica un importante avance a la hora de superar situaciones de interrupción de las actividades y servicios prestados por la Unidad de Tecnologías de la Información. Es indispensable para el éxito del Plan de Contingencia contar con el personal involucrado capacitado y comprometido con la continuidad de las operaciones.

II. DOCUMENTOS DE REFERENCIA

2.1. Norma Técnica Peruana NTP ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

2.2. Resolución Ministerial N° 028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno.

2.3. Resolución de Dirección Ejecutiva N° 244-2018-MIDIS/PNAEQW, que aprueba el Manual de Gestión de Riesgos.

III. DEFINICIONES

3.1. Activo de información: Comprende a cada elemento que soporta la información, es decir que la contiene, la procesa y la transporta.

3.2. Amenaza: Causa potencial de un incidente no deseado.

3.3. Contingencia: Situación incierta de impacto negativo que puede ocurrir o no en un futuro.

3.4. Impacto: Resultado de un suceso o evento de contingencia.

3.5. Probabilidad: Posibilidad de que algún evento de contingencia se materialice.

3.6. Riesgo: Incertidumbre que podría desencadenar una interrupción indeterminada en los servicios de TI.

3.7. Riesgo Operativo: Riesgo vinculado a la administración y supervisión del personal.

3.8. Riesgo Técnico: Riesgo vinculado fallas en los suministros de energía y servicios complementarios.

3.9. Riesgo Tecnológico: Riesgo vinculado a los servicios de tecnologías de la información.

3.10. Servicio crítico: Servicio de gran valor para el cumplimiento de los objetivos del PNAEQW.

3.11. UPS: Dispositivo alterno de almacenamiento de energía eléctrica.

3.12. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

IV. DIAGNÓSTICO

4.1. Equipo de Contingencia de TI

a. Uno de los aspectos que evidencia un carácter formal y serio en toda entidad es que se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria, mientras dure dicho evento.

b. Es necesario entonces que el Plan de Contingencia de TI deba hacerse de manera formal y responsable involucrando a toda la entidad en los Planes de Prevención, Ejecución y Recuperación[1], pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

Equipo de Contingencia de TI

Dirección Ejecutiva del PNAEQW

Jefatura de la Unidad de Tecnologías de la Información

Grupo Operativo de UTI
- ✓ Oficial de Seguridad de la Información o quien haga sus veces.
- ✓ Especialista en administración de Data Center o quien haga sus veces.
- ✓ Especialista en redes y comunicaciones o quien haga sus veces.
- ✓ Administrador de Base de Datos o quien haga sus veces.
- ✓ Personal de desarrollo de sistemas o quien haga sus veces.
- ✓ Web Master o quien haga sus veces.
- ✓ Personal de soporte técnico o quien haga sus veces.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA V°B° JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN MIDIS

E. MORALES F.

[1] Estos planes se encuentran desarrollados en la parte estratégica del presente plan.

4.2. Responsabilidades

a. La Dirección Ejecutiva es responsable de:
   - Aprobar el Plan de Contingencia de TI.
   - Ordenar la ejecución del Plan de Contingencia de TI
   - Brindar los recursos necesarios para el correcto desempeño del Plan de Contingencia de TI.

b. La Jefatura de la Unidad de Tecnologías de la Información es responsable de:
   - Presentar a la Dirección Ejecutiva la propuesta del Plan de Contingencia de TI.
   - Informar a la Dirección Ejecutiva sobre la materialización del evento de contingencia y sus resultados.
   - Activar/Desactivar la ejecución del Plan de Contingencia de TI.
   - Informar a las Unidades afectadas sobre la ocurrencia del evento de contingencias y coordinar las acciones necesarias.
   - Supervisar la ejecución de las actividades del Plan de Pruebas.

c. El Oficial de Seguridad de la Información es responsable de:
   - Elaborar, revisar y mantener actualizado el Plan de Contingencias de TI.
   - Ejercer control y seguimiento del Plan de Contingencia de TI.
   - Coordinar la ejecución del Plan de Contingencia de TI.
   - Informar a la Jefatura de TI sobre los resultados obtenidos en el Plan de Contingencia de TI
   - Coordinar simulacros periódicos en relación al Plan de Pruebas con el fin de mantener activos a los miembros del equipo y la vigencia del Plan Contingencia de TI.
   - Verificar que el personal involucrado este permanentemente capacitado respecto a su función dentro del Plan de Contingencia de TI.

d. Grupo Operativo de UTI es responsable de:
   - Ejecutar las actividades operativas descritas en el presente Plan.

4.3. Valoración de Criticidad

El nivel de criticidad de los sistemas de información, servicios tecnológicos y componentes informáticos de software y hardware que administra la Unidad de Tecnologías de la Información se valorarán conforme a los siguientes criterios:

NIVEL	DESCRIPCIÓN
ALTO	Afecta directamente en los procesos de negocio y de soporte del PNAEQW, y es causal de la paralización indeterminada de las operaciones. Adicionalmente Impacta negativamente en la imagen institucional.
MEDIANO	Afectar las operaciones en algunas Unidades orgánicas del PNAEQW, no afectando indeterminadamente a los procesos de negocio y no impacta negativamente a la imagen institucional.
BAJO	No causa un efecto considerable en el PNAEQW.

4.4. Sistemas de Información y Aplicativos

El inventario de los servicios de sistemas de información y aplicativos que cuenta la Unidad de Tecnologías de la Información está constituido por lo siguiente:

N°	SISTEMA DE INFORMACIÓN Y APLICATIVOS	DESCRIPCION	CRITICIDAD
1	SISTEMA INTEGRADO DE GESTIÓN OPERATIVA SIGO v.15	Solución web que atiende procesos operativos de las Unidades Técnicas y Unidades Territoriales del PNAEQW. Lo integran módulos y aplicativos para las diferentes Unidades Orgánicas de línea del PNAEQW.	ALTO
2	SISTEMA INTEGRADO DE GESTIÓN ADMINISTRATIVA SIGA	Solución de escritorio que atiende procesos administrativos de gestión logística y control patrimonial que opera en la Unidad de Administración del PNAEQW Sede Central.	ALTO
3	SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA SIAF	Solución de escritorio que atiende procesos administrativos de gestión financiera que opera en la Unidad de Administración del PNAEQW Sede Central.	ALTO
4	SISTEMA DE GESTIÓN DE INFORMACIÓN INTERNA INTRANET	Solución Web para gestión de información interna.	MEDIO
5	SISTEMA DE GESTIÓN DE INFORMACIÓN EXTERNA PÁGINA WEB	Solución Web para gestión de información externa.	MEDIO
6	SISTEMA DE ADMINISTRACIÓN DE RECURSOS HUMANOS SARH	Solución de escritorio que atiende procesos de administración de recursos humanos.	MEDIO
7	SISTEMA DE BOLSA DE TRABAJO PNAEQW	Solución Web que atiende el proceso de convocatoria de personal y registro de postulantes a las oportunidades laborales del PNAEQW.	BAJO
8	SISTEMA DE CONTROL DE ASISTENCIA DE PERSONAL TEMPUS	Solución Informática para control de asistencia de personal.	BAJO
9	SISTEMA DE GENERACIÓN DE REPORTES MELISSA V2.0	Herramienta Informática para generación de reportes financieros del SIAF.	MEDIO
10	SISTEMA DE REGISTRO DE CONTROL DE VISITAS	Herramienta informática que permite registrar los datos de visitantes a funcionarios del PNAEQW, es una solución desarrollada por la PCM.	BAJO
11	SISTEMA DE CONTROL DE TRÁMITE DOCUMENTARIO SITRADOC	Solución Web que atiende el proceso de Gestión del Trámite Documentario, ha sido desarrollada por el MIDIS.	MEDIO
12	SISTEMA DE INFORMACIÓN DE INDICADORES DE GESTION – INFO QALIWARMA	Solución Web que permite mostrar información de los indicadores de gestión del proceso del servicio alimentario. Su acceso es a través del portal web.	BAJO

13	SIGO PROVEEDORES	Plataforma que permite visualizar los registros de entregas de alimentos realizados desde el Aplicativo Móvil QW PROVEEDORES	ALTO
14	SIGO POSTORES	Plataforma que permite registrar participantes para las convocatorias del Proceso de Compras 2018.	ALTO
15	PLATAFORMA DE ATENCIÓN AL USUARIO	Solución Web que reemplaza a SIGMAD y que permite registrar las ocurrencias presentadas durante el uso del Sistema Integrado de Gestión Operativa – SIGO, Sistema de Trámite Documentario – SITRADOC y el Sistema de Administración y Expedientes Digitales – SADE.	BAJO
16	QW PROVEEDORES	Aplicativo móvil que permite al proveedor registrar las entregas de productos y raciones realizadas en las Instituciones Educativas públicas afiliadas al PNAE Qali Warma.	ALTO
17	QW ESTABLECIMIENTOS	Aplicativo móvil usado por los Supervisores de Plantas y Almacenes durante la evaluación a los establecimientos de los postores y proveedores a nivel nacional.	ALTO
18	QW RUTAS	Aplicativo móvil que permite sistematizar la actividad de acompañamiento al proveedor en su ruta de distribución de productos o raciones.	ALTO
19	QW IIEE	Aplicativo móvil que sistematiza la actividad de supervisión a cada una de las etapas de la prestación del servicio alimentario en las Instituciones Educativas afiladas al PNAE Qali Warma.	ALTO

4.5. Servicios Tecnológicos

N°	NOMBRE DEL SERVICIO	DESCRIPCIÓN	CRITICIDAD
1	DIRECTORIO ACTIVO	Servicio de administración de inicios de sesión en los equipos conectados a la red del PNAEQW, así como también la administración de políticas en toda la red.	ALTA
2	ACCESO A INTERNET	Servicio de internet del PNAEQW	ALTA
3	INTRANET	Servicio de administración de información y recursos internos a la red del PNAEQW.	MEDIA
4	PAGINA WEB	Servicio de administración de información y recursos de carácter público.	ALTA
5	CORREO ELECTRONICO	Servicio de mensajería electrónica del PNAEQW	MEDIA
6	SOPORTE TECNICO	Servicio de soporte técnico del PNAEQW	MEDIA

4.6. Software y Respaldo de Información

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	CRITICIDAD
1	SOFTWARE	Para este activo se refiere: base de datos y desarrollo, antivirus, sistemas operativos, ofimática, software para monitoreo	ALTA
2	RESPALDO DE INFORMACIÓN	Activos de respaldo para: base de datos, sistemas de información, portal web y archivos, configuración.	ALTA

4.7. Hardware y Comunicaciones

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	CRITICIDAD
1	REDES Y COMUNICACIONES	Servidores físicos Switch Router Firewall UPS Cableado estructurado	ALTA
2	SISTEMAS DE APOYO	Sistema de aire acondicionado Sistema de energía eléctrica	ALTA

4.8. Descripción de los Eventos de Contingencias

TIPO		EVENTO	DESCRIPCIÓN
Externo	Tecnológico	Caída o interrupción de energía eléctrica - (E1)	Corresponde al corte del servicio de energía eléctrica en la Sede Central del PNAEQW ubicado en Av. Circunvalación Golf Los Inkas 206-208, corte eléctrico que genera interrupción del funcionamiento de los servidores donde se alojan los sistemas de información y/o aplicaciones del PNAEQW. Esta situación impacta en la disponibilidad de los servicios de TI.
		Infección masiva por software malicioso – (E3)	Es el riesgo de infección de los equipos de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de las unidades de trabajo.
	Operativo	Suspensión de las actividades por sismo, inundación o incendio – (E4)	Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo o incendio que afecte la infraestructura tecnológica del PNAEQW generando suspensión total o parcial del funcionamiento del Centro de Datos o de la prestación de servicios de TI. Tipo de riesgo: Operativo.
	Técnico	Caída de internet – (E2)	Consiste en las fallas técnicas por parte del proveedor del servicio de internet en la Sede Central del PNAEQW ubicado en Av. Circunvalación Golf Los Inkas 206-208, lo que ocasionaría suspensión de los servicios de TI incluyendo correo, red, sistemas y aplicativos de información del PNAEQW.
Interno	Tecnológico	Falla técnica en equipos servidores– (E6)	Corresponde al daño físico o lógico de un equipo servidor, que afecta el funcionamiento de un sistema de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o inestable. Tipo de riesgo: Tecnológico.
		Falla técnica en Sistemas de Información critico – (E7)	Representa una falla técnica en alguna funcionalidad de los sistemas de información y aplicativos críticos del PNAEQW que se vea afectada la integridad de la información en el continuo uso de los mismos. Tipo de riesgo: Tecnología.
	Operativo	Accesos no autorizados al Centro de Datos del PNAEQW – (E5)	Consiste en el acceso al Centro de Datos de personal no autorizadas que pueden ocasionar sabotaje, robo, alteración o extracción de información que es considerada confidencial o clasificada, así como también el daño a los componentes informáticos. El impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional.

		Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes – (E8)	Corresponde a la falta o inasistencia en un momento dado, de un trabajador crítico de la UTI que realiza actividades de soporte a usuarios sobre un sistema de información crítico del PNAEQW por enfermedad, epidemia muerte o incapacidad, lo que genera inoperancia o inestabilidad de los sistemas de información, servidores y redes. Tipo de Riesgo: Operativo.
	Técnico	Calentamiento del centro de datos – (E9)	Consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos. Tipo de riesgo: Tecnología.

4.9. Valoración de los Eventos de Contingencia

La determinación del impacto, probabilidad y del evento de contingencia se realizarán según lo establecido en el documento normativo MAN-008-PNAEQW-UPPM, Manual de Gestión del Riesgo del PNAEQW.

Los eventos de contingencia que se tomarán como prioridad para el desarrollo del presente Plan de Contingencia de TI serán los catalogados como "INACEPTABLE" E "IMPORTANTE", es decir aquellos que puedan afectar drásticamente la continuidad de los servicios de TI. Para los valores de "MODERADO", "TOLERABLE" y "ACEPTABLE" no serán abordados en el presente Plan.

En función a ello, los eventos de contingencia descritos en el numeral 4.8 precedente, tienen la siguiente valoración:

N°	EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN
E1	Caída o interrupción de energía eléctrica	Improbable	Catastrófico	[redacted]
E2	Caída de internet	Posible	Mayor	
E3	Infección masiva por software malicioso	Improbable	Catastrófico	
E4	Suspensión de las actividades por sismo, inundación o incendio	Improbable	Catastrófico	
E5	Accesos no autorizados al Centro de Datos del PNAEQW	Improbable	Mayor	MODERADO
E6	Falla técnica en equipos servidores, de escritorio o de comunicaciones	Posible	Mayor	[redacted]
E7	Falla técnica en Sistemas de Información critico	Posible	Mayor	
E8	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información y comunicaciones	Posible	Moderado	
E9	Calentamiento del centro de datos	Posible	Mayor	

VºBº JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN

B. MORALES F.

V. OBJETIVOS

5.1. Objetivo General

Garantizar la continuidad de los servicios de TI de la Sede Central del PNAEQW soportados por la infraestructura tecnológica de la Unidad de Tecnología de Información.

5.2. Objetivos Específicos

a. Contar con un documento de utilidad para afrontar algún evento de contingencia que afecte los servicios críticos de TI del PNAEQW.
b. Prevenir los posibles eventos de contingencia promoviendo las revisiones técnicos de los componentes de la plataforma tecnológica.
c. Organizar al grupo operativo de la Unidad de Tecnología de la Información identificando sus roles y responsabilidades.

VI. RESULTADOS ESPERADOS

6.1. El presente Plan de Contingencia de TI buscar restablecer los servicios de TI en un margen aceptable no menor al 95% de su capacidad de restauración.

VII. ALCANCE

7.1. El presente documento aplica a la continuidad operativa de los servicios de TI en la Sede Central del PNAEQW, soportados por los equipos e infraestructura tecnológica de la Unidad de Tecnologías de la Información.

VIII. ESTRATEGIAS

8.1. Planes de Contingencia

Desarrollaremos las estrategias relacionadas con cada evento o incidente que provoque alto impacto en la continuidad de los servicios de TI de la UTI. Para lo cual se está dividiendo en 3 partes:

a. **Prevención:** Mecanismos para prevenir dichos eventos antes de que sucedan; ayudan a reducir el impacto y estar siempre preparados ante eventualidades de desastres.
b. **Ejecución:** Después de iniciado el evento y ayuda a la recuperación de las funciones críticas, se considera los tiempos de continuidad.
c. **Recuperación:** Procedimientos para retomar las actividades ya recuperadas en su lugar de origen.

PNAEQW	Evento: Caída o interrupción de energía eléctrica - (E1)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Falla general del suministro de energía eléctrica. Este evento incluye los siguientes elementos mínimos identificados por el PNAEQW, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

- Servicios Públicos
- Suministro de Energía Eléctrica
- Hardware
- Servidores
- Estaciones de Trabajo
- Equipos Diversos
- UPS

1.2. Objetivo

Restablecer energía eléctrica en el Centro de Datos del PNAEQW ante un evento de contingencia para asegurar la continuidad operativa de los sistemas críticos de TI.

1.3. Valoración

Este evento es considerado de alto impacto.

1.4. Entorno

Se delimita al Centro de Datos ubicado de la sede Central del PNAEQW.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center.

1.6. Condiciones de Prevención de Riesgo

- Verificar que durante las operaciones diarias de servicio u operaciones del PNAEQW se contará con los UPS necesarios para asegurar el suministro eléctrico en el Centro de Datos del PNAEQW.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 4 horas como mínimo.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Corte de suministro de energía en la Sede Central del PNAEQW por un tiempo mayor a 30 minutos.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones de la sede principal del PNAEQW.

2.3. Personal que autoriza la Contingencia

- Jefa o Jefe de la Unidad de Tecnologías de la Información.

2.4. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Informar a la Jefatura de la Unidad de Tecnologías de la Información sobre el evento presentado.
- Verificar la activación automática de los UPS.
- Comunicar a todas las Unidades Orgánicas del PNAEQW del evento y coordinar las acciones necesarias.
- En caso la interrupción de energía sea mayor a 4 horas se deberá apagar los servidores que alojen los sistemas y aplicaciones críticos del PNAEQW hasta el retorno del fluido eléctrico.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA V°B° JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN MIDIS

- Monitorear el uso de equipos UPS para el restablecimiento de energía en los servidores de soporte a los sistemas críticos.
- Evaluar la provisión de un servicio externo de energía eléctrica temporal (grupo electrógeno).
- Coordinar con las Unidades Orgánicas afectadas de tomar las medidas necesarias ante la activación del Plan de Contingencia de TI.

2.6. Duración
El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía.

3. PLAN DE RECUPERACIÓN

3.1. Personal operativo encargado
- Especialista de administración de Data Center
- Especialista en redes y comunicaciones
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades
- Verificar el estado de la infraestructura tecnológica impactada por el evento.
- Verifica el restablecimiento de la energía eléctrica y el funcionamiento del Centro de Datos.
- Analizar la necesidad de usar las copias de respaldo y backups.
- Verificar el restablecimiento de los sistemas críticos de información.
- Comunicar a las Unidades Orgánicas afectadas el restablecimiento de los sistemas de información críticos
- Elaborar un informe a la Jefatura de la Unidad de Tecnologías de la Información sobre el problema presentado y el procedimiento usado para atender el evento.
- Registrar aquellas actividades que sirva para actualizar el Plan de Contingencia de TI en caso vuelva a presentarse dicha eventualidad.
- Registrar el evento en el Formato Registro de Contingencias

3.3. Mecanismo de comprobación
- Comunicar a todas las Unidades Orgánicas del PNAEQW a fin de constatar el correcto funcionamiento de los sistemas de información críticos en cada unidad de trabajo.
- Garantizar la funcionalidad de las instalaciones eléctricas en la Sede Central del PNAEQW.

3.4. Desactivación del Plan de Contingencia de TI
La Jefa o Jefe de la Unidad de Tecnologías de la Información desactivará el Plan de Contingencia una vez se haya restablecido la energía eléctrica al Centro de Datos y los servicios de TI.

3.5. Proceso de actualización del Plan
Se tomaran las recomendaciones formuladas en los informes presentados a la Jefatura de la Unidad de Tecnologías de la Información para la presente contingencia.

PNAEQW	Evento: Infección masiva por software malicioso – (E3)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Los softwares maliciosos son programas informáticos que se propagan de un equipo a otro y que interfieren en su correcto funcionamiento. Además, pueden dañar o eliminar los datos de un equipo. Este evento incluye los siguientes elementos mínimos identificados por el PNAEQW, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:
- Servidores.
- Estaciones de trabajo (PC y Laptops).
- Software base datos.
- Aplicativos y sistemas de información del PNAEQW.

1.2. Objetivo
Restaurar la operatividad de los activos informáticos después de eliminar el software malicioso que causa la contingencia.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Los activos informáticos (PC, Laptops, servidores y sistemas de información) de la Sede Central del PNAEQW.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Soporte Técnico o quien haga sus veces.

1.6. Condiciones de prevención de riesgos
- Establecer políticas y normativas de seguridad que regulen el uso adecuado de los activos de información
- Utilizar mecanismos de seguridad que restringa el acceso a páginas de internet de contenido malicioso.
- Restringir el acceso a las grabadoras de CD y USB en las estaciones de trabajo que no lo requieran.
- Aplicar filtros para restricción de correo entrante y así prevenir la infección de los terminales de trabajo por virus.
- Verificar que el antivirus instalado en cada estación de trabajo deba estar actualizado permanentemente.
- Verificar que los sistemas operativos cuenten con los parches de actualización.
- Escanear la red constantemente a fin de identificar instalaciones de agentes maliciosos.
- Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.
- Capacitar y concientizar al personal del PNAEQW sobre temas de seguridad de la información.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
- Mensajes de error durante la ejecución de los sistemas de información y aplicaciones.
- Lentitud o paralización de los sistemas de información y aplicaciones.
- Falla general en los activos de informáticos (PC, Laptops, servidores y sistemas de información)

2.2. Procesos relacionados antes del evento
Cualquier proceso relacionado con el uso de sistemas y aplicaciones en las estaciones de trabajo.

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Unidad de Tecnologías de la Información.

2.4. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Soporte técnico o quien haga sus veces.

2.5. Descripción de actividades
- Desconectar preventivamente el equipo infectado de la red de PNAEQW.
- Verificar la infección del equipo afectado y el alcance del mismo.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Eliminar el agente viral causante de la infección.
- Escanear la red del PNAEQW en virtud de eliminar posibles agentes virales informáticos.
- En caso no solucionarse el problema:
  - Formatear el equipo
  - Personalizar la estación para el usuario.
- Conectar la estación a la red del PNAEQW.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

2.6. Duración

La duración del evento no deberá ser mayor a 6 horas en caso se confirme la presencia de un software malicioso.
Los usuarios deberán esperar las indicaciones del personal de soporte para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Soporte técnico o quien haga sus veces.

3.2. Descripción de actividades
- Registrar la conformidad del usuario una vez se haya eliminado la amenaza de virus en su estación de trabajo.
- Realizar pruebas de funcionamiento en las estaciones de trabajo (Sistemas de información, servicios tecnológicos y aplicaciones del PNAEQW).
- Coordinar con el usuario responsable el procedimiento para reanudar las labores normales en el ambiente de trabajo original.
- Dar indicaciones de seguridad y prevención a los usuarios.
- Recomendar capacitación a la UTI de ser necesario
- Realizar informe de las acciones tomadas durante el evento.

Se informará a la Jefatura de la Unidad de Tecnología de la Información el tipo de software malicioso encontrado y el procedimiento usado para removerlo. En función a esto, se tomarán las medidas preventivas del caso.
El evento será evaluado y registrado en el formato de registro de contingencia.

3.3. Mecanismo de comprobación
- Asegurar que el antivirus funcione correctamente y se encuentre en constante actualización.
- Verificar que el Sistema Operativo se encuentre con las actualizaciones y parches.

3.4. Desactivación del plan de continuidad
La Jefa o Jefe de la Unidad de Tecnologías de la Información desactivará el presente Plan una vez se haya eliminado la amenaza.

3.5. Proceso de actualización
En base al informe presentado que identifica las causas de la infección de virus informático, se determinará las acciones preventivas necesarias que deberán incluirse en el presente Plan.

PNAEQW	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Constituye la situación en la que el Centro de Datos del PNAEQW se encuentra declarada inhabitable, producto de un desastre de mayores magnitudes, pudiendo provocar derrumbe de la infraestructura, perdida de materiales, recursos informáticos y humanos.
Las causas que pueden provocar este evento encontramos las siguientes:

Incendio: 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.

Sismo de gran intensidad en Lima: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento errático del terreno.

Inundación: Flujo descontrolado de agua producto de lluvias torrenciales o fugas y/o daños en el sistema hidráulico.

1.2. Objetivo
Establecer las acciones que se tomarán ante un incendio, inundación o sismo de grandes magnitudes a fin de minimizar el tiempo de interrupción de los servicios criticos de TI.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Este evento se localiza en las instalaciones del Centro de Datos de la sede central del PNAEQW.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Especialista en redes y comunicaciones.

1.6. Condiciones de prevención de riesgos

Incendio de grandes magnitudes en uno o más ambientes:

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Asistir a charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Acatar las indicaciones de Defensa Civil, en torno al evento.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal responsable de las acciones de prevención y ejecución de la contingencia.
- Verificar el funcionamiento de los detectores de humo en el Centro de Datos del PNAEQW.

Sismo de gran intensidad en Lima
- Contar con un plan de evacuación de las instalaciones del PNAEQW, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realizar simulacros de evacuación con la participación de todo el personal del PNAEQW.
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

Inundaciones de grandes magnitudes
- Verificar que las instalaciones hidráulicas del PNAEQW se encuentren en correcto estado y en mantenimiento continuo.
- Posicionar los activos estratégicos del Centro de Datos en plataformas elevadas.
- Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
El proceso de contingencia se activara inmediatamente después de ocurrido los eventos descritos en el punto 1.1.

2.2. Actividades relacionados antes de los eventos detonantes
- Identificar la ubicación de las estaciones manuales de alarma contra incendio.
- Identificar la ubicación de los extintores.
- Conocer el grupo de brigadistas asignados por el PNAEQW.
- Conocer el número de emergencia de los bomberos.
- Inspecciones regulares de seguridad interna.
- Inspecciones regulares de seguridad externa.
- Participación en simulacros internos.

2.3. Personal que autoriza la Contingencia
Dirección ejecutiva del PNAEQW en coordinación con la Jefatura de la Unidad de Tecnologías de la Información.

2.4. Personal encargado Operativo
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Especialista en redes y comunicaciones.
- Administrador de base de datos o quien haga sus veces.

V°B° JEFA DE LA UNIDAD DE TÉC. DE LA INFORMACIÓN

- Personal de desarrollo de sistemas o quien haga sus veces.
- Web Master o quien haga sus veces.

2.5. Descripción de actividades para la restauración del Centro de Datos
- Evaluar los daños ocasionados en el Centro de Datos del PNAEQW.
- Verificar la disponibilidad del espacio físico asignado para el Centro de Datos alterno del PNAEQW.
- Trasladar el Centro de Datos asegurando que las características ambientales necesarias para su implementación sean óptimas.
- Asegurar las condiciones eléctricas y de refrigeración mínimas para el funcionamiento del Centro de Datos provisional.
- Considerar la adquisición de equipamiento tecnológico que asegure la disponibilidad del Centro de Datos provisional.
- Configurar la infraestructura tecnológica que soporte el levantamiento de los sistemas de información críticos del PNAEQW.
- Coordinar el traslado seguro de las copias de seguridad en custodia por el proveedor al nuevo ambiente de físico del Centro de Datos.
- Restaurar las copias de seguridad de los sistemas de información del PNAEQW.
- Ejecutar las pruebas necesarias para asegurar la disponibilidad de los servicios críticos de TI.
- Informar a la Jefatura de la Unidad de Tecnologías de la Información el restablecimiento del Centro de Datos provisional del PNAEQW.

2.6. Duración
El proceso de evacuación del personal de la Sede Central del PNAEQW tomara un tiempo no mayor a 5 minutos.

El proceso de implementar un Centro de Datos provisional (de ser necesario) tomara un tiempo no mayor a 12 horas

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

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Especialista en redes y comunicaciones.
- Administrador de base de datos o quien haga sus veces.

3.2. Descripción de actividades
- Verificar los daños a los componentes informáticos del Centro de Datos principal.
- Realizar el inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de los mismos.
- Trasladar hacia el Centro de Datos alterno provisional los componentes informáticos en buen estado.
- Habilitar los muebles y logística necesaria para su operatividad.
- Garantizar la habilitación del servicio de fluido eléctrico.
- Reinstalación del personal critico de TI.
- Monitorear constantemente la funcionalidad de los servicios críticos de TI.

3.3. Mecanismo de comprobación
Elaborar un informe a la Jefatura de Tecnologías de la Información detallando los daños afectados a los activos de Información críticos del PNAEQW y las acciones tomadas.
Se llenara el formato de ocurrencia de eventos para este fin.

3.4. Desactivación del Plan de Recuperación
Se desactivara una vez se tome por superado el desastre y se retome las actividades de origen.

3.5. Proceso de actualización
El proceso de actualización será en base al informe presentado a la Dirección Ejecutiva a efectos que determine las acciones a tomar.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA - MIDIS
VºBº
JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN

PNAEQW	Evento: Falla técnica en servidores – (E6)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Falla técnica de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del PNAEQW.

1.2. Objetivo
Asegurar la continuidad y operatividad de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del PNAEQW.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Servidores de soporte para los servicios críticos de TI, sistemas de información y aplicaciones localizados en el Centro de Datos del PNAEQW.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.
- Administrador de base de datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo
- Revisión periódica técnica de los servidores del Centro de Datos.
- Mantener actualizada la garantia de equipos y servidores vigentes.
- Copias de seguridad de los sistemas de información y aplicaciones del PNAEQW.
- Monitoreo periódico de red del PNAEQW.
- Seguridad periférica.
- Protección física adecuada al Centro de Datos.
- Mecanismos de seguridad y controles de acceso.
- Adecuada ventilación y refrigeración en el Centro de Datos.
- Procedimientos para el uso correctos de los activos de información.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
- Fallas en la conexión, servidores no responden.
- Indisponibilidad de uso de los sistemas y aplicativos del PNAEQW.

2.2. Procesos relacionados antes del evento
- Tener las copias de respaldo disponibles para su aplicación en los servidores de contingencia del PNAEQW.
- Traslado de las copias de seguridad del proveedor de custodia a la Sede Central del PNAEQW.

2.3. Personal encargado
- Oficial de seguridad de la Información.
- Especialista en administración de Data Center.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

2.4. Descripción de los procedimientos después de activar la contingencia:
- Analizar la causa resultante o disparador del evento.
- Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del PNAEQW.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de los servicios de TI.
- Comunicar a los proveedores del servidor e informar la incidencia.
- Desconectar de la red el servidor afectado.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA
V°B°
JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN
MIDIS

- Activar y configurar el equipo necesario de contingencia para el levantamiento de los servicios de TI en los servidores alternos de contingencia.
- Ejecutar las restauraciones de los sistemas y aplicaciones críticos en los servidores alternos de contingencia en caso se requiera.
- Realizar las pruebas de funcionamiento.
- Comunicar a los usuarios el restablecimiento de los servicios de TI.

2.5. Duración
Duración de 4-5 horas.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Especialista en administración de Centro de Datos.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades
- Conectar a la red el equipo inicial reparado.
- El Especialista en Administración de Centro de Datos verifica el correcto desempeño de los servidores reparados y de los sistemas de información críticos que soportan.
- Se informará a la Jefatura de Unidad de Tecnologías de la Información la causa del problema presentado y el procedimiento usado para atender el problema. En función a esto, se tomarán las medidas preventivas del caso.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

3.3. Mecanismos de Comprobación
- Una vez identificada el origen de la falla de los servidores que ocasionó el evento, se deberá realizar un informe técnico detallado y consolidando las acciones tomadas.
- Revisar las configuraciones y programar con el proveedor de los equipos, revisiones periódicas a fin de reducir la amenaza que vuelva a suceder.

3.4. Desactivación del Plan de Contingencia
La Jefa o Jefe de la Unidad de Tecnologías de la Información desactivará el Plan de Contingencia una vez que el especialista en administración de Data Center informe la operatividad de los servidores.

3.5. Proceso de actualización
El proceso de actualización será en base al informe presentado a la Dirección Ejecutiva quien determinará las acciones a tomar.

PNAEQW	Evento: Falla en Sistemas de Información críticos – (E7)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Es el uso defectuoso de los sistemas de información críticos del PNAEQW, haciendo que el uso de estos corresponda a un elevado riesgo en la integridad de la información que se procese o simplemente este último deje de funcionar.

1.2. Objetivo
Restaurar el funcionamiento de los sistemas de información y aplicaciones críticos del PNAEQW.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Sistemas de información y aplicativos críticos del PNAEQW.

1.5. Personal encargado
- Oficial de seguridad de la información
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA VºBº JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN MIDIS

V 5°

1.6. Condiciones de Prevención de Riesgo
- Copia de seguridad de la información críticos para asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos relacionadas.
- Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante y licencias vigentes.
- Evitar el uso de software no licenciado que pueda estar corrupto
- Revisión preventiva de los sistemas y mantenimiento general de las bases de datos.
- Directivas o procedimiento de desarrollo seguro.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
Fallas en el uso de los sistemas de información que generen su inutilidad.
Información procesada no cuenta con integridad y fiabilidad.

2.2. Procesos relacionados antes del evento
Respaldo disponible de los sistemas de información críticos.

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Unidad de Tecnologías de la Información del PNAEQW.

2.4. Personal encargado
- Oficial de seguridad de la información
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

2.5. Descripción de las actividades después de activar la contingencia:
- Desconectar de la red el equipo afectado.
- Configurar equipo de respaldo para el sistema de información o aplicación crítica afectada.
- Restaurar la copia de seguridad más reciente del aplicativo critico correspondiente.
- Crear los permisos a cada carpeta compartida.
- Verificar la existencia del servidor nuevo en el dominio y colocarlo en producción.
- Informar a los usuarios la nueva ruta del servidor del aplicativo

2.6. Duración
El tiempo máximo de duración de la contingencia será dependiendo de la causa que originó la contingencia.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Centro de Datos.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades
- Revisar el sistema de Información o aplicativo dañado para determinar la falla o error lógico presentado.
- Hacer pruebas al sistema de Información o aplicativo una vez entregada la solución por el proveedor, en ambiente de pruebas.
- Realizar copia de la base de datos del sistema de Información o aplicativo que está en funcionamiento como contingencia.
- Restaurar la copia de seguridad más reciente del aplicativo afectado en el servidor inicial.
- Verificar los permisos sobre el sistema de información o aplicativo.
- Informar a los usuarios la ruta del servidor del sistema de información o aplicativo.
- Conectar a la red el equipo inicial reparado.

3.3. Mecanismos de comprobación
El Especialista en administración de Centro de Datos presentara un informe a la Jefatura de la Unidad de Tecnologías de la Información explicando que servicio ha sido afectado y cual son las acciones tomadas.

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Unidad de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización
En base al informe presentado a la Jefatura de Unidad de Tecnologías de la información y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

PNAEQW	**Evento: Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes– (E8)**	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Ausencias del personal (enfermedad, epidemias, renuncias masivas, ceses), critico que brinda soporte y mantenimiento a los sistemas de información, servidores y redes que mediante su ausencia pueda originar paralización en las operaciones del PNAEQW.

1.2. Objetivo
Reemplazar al personal crítico ausente con elementos capacitados que puedan cubrir sus funciones hasta la inserción o reemplazo del ausente.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Unidad de Tecnologías de la Información.

1.5. Personal encargado
- Jefa o Jefe de la Unidad de Tecnologías de la Información.
- Oficial de seguridad de la información.

1.6. Condiciones de Prevención de Riesgo
- Asegurar la capacitación adecuada de los Analistas de Sistemas con el fin de que cumplan con el perfil, conocimiento y capacidad de reemplazar la ausencia de los administradores de sistemas y redes del PNAEQW.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labor.
- Elaborar diccionarios de datos y/o manuales de uso para facilitar las actividades del reemplazante.
- Programar chequeos preventivos médicos al personal crítico en periodos semestrales o anuales.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
Inasistencia no premeditada del personal crítico (administrador de sistemas y redes).

2.2. Procesos relacionados antes del evento
La Jefatura de la Unidad de Tecnologías de la Información tiene conocimiento de inasistencia del personal crítico.

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Unidad de Tecnologías de la Información del PNAEQW.

2.4. Personal encargado
- Oficial de seguridad de la información.

2.5. Descripción de las actividades después de activar la contingencia:
- Confirmada la inasistencia del personal, la Jefatura de la Unidad de Tecnologías de la Información asignara al reemplazo provisional del personal ausente.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA V°B° JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN MIDIS

V°B°

- Poner a disposición los recursos necesarios para que el personal suplente lleve a cabo sus actividades efectivamente.

2.6. Duración
El tiempo máximo de duración de la contingencia será dependiendo de la causa que originó la ausencia temporal.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
La Jefa o Jefe de la Unidad de Tecnologías de la Información

3.2. Descripción de actividades
- Facilitar el reinserción del personal ausente
- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

3.3. Mecanismos de comprobación
Informes de desempeño laboral cuando sea requerido por la Jefatura de la Unidad de Tecnologías de la Información

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Unidad de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización
En base al informe presentado a la Jefatura de Unidad de Tecnologías de la información y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

PNAEQW	Evento: Calentamiento del Centro de Datos – (E9)	UTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Aumento de temperatura dentro del Centro de Datos y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades del PNAEQW.

1.2. Objetivo
Restaurar los servicios críticos de TI que soportan los servidores del Centro de Datos.

1.3. Valoración
Este evento es considerado de alto impacto.

1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del PNAEQW.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.

1.6. Condiciones de Prevención de Riesgo
- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con un sistema adecuado de ventilación en el Centro de Datos.
- Contar con mantenimiento preventivo para los equipos de ventilación o aire acondicionado.
- Contar con backups de información y aplicaciones necesarios.
- Almacenar en un lugar seguro, de ser posible externo, los backups de información y aplicaciones.
- Libreta de números de contacto del proveedor al alcance.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA
V°B°
JEFA DE LA UNIDAD DE TEC. DE LA INFORMACIÓN
-MIDIS-

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
- Falla del sistema de ventilación del Centro de Datos
- Falla de los servicios criticos del PNAEQW

2.2. Procesos relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones del PNAEQW.

2.3. Personal que autoriza la Contingencia
- La Jefa o Jefe de la Unidad de Tecnologías de la Información del PNAEQW.

2.4. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.

2.5. Descripción de los procedimientos después de activar la contingencia:
- Verificar la magnitud del fallo o avería al sistema de ventilación del Centro de Datos.
- Notificar al proveedor de aire acondicionado sobre la magnitud de fallos o averia.
- Instalar equipos de ventilación de contingencia.
- Apagar los equipos electrónicos innecesarios.
- Restablecer el sistema de ventilación del Centro de Datos.

2.6. Duración
El tiempo máximo de duración de la contingencia dependerá del proveedor del sistema de ventilación.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center.

3.2. Descripción de actividades
- El especialista de administración de Data Center revisara que el sistema de ventilación haya sido reparado y funcione con normalidad.
- El proveedor del sistema de ventilación una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informara a la Jefatura de la Unidad de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación
La UTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de ventilación del Centro de Datos se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Unidad de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización
En base al informe presentado por el proveedor del sistema de ventilación de Centro de Datos se tomaran las acciones correctivas para la actualización del Plan de Contingencia.

IX. ACTIVIDADES

9.1. Las actividades de los planes de contingencias se describen en los títulos "Descripción de Actividades" del Punto VI.

X. CRONOGRAMA

10.1. **Plan de Pruebas:** El Plan de Contingencias de TI comprende, el desarrollo de un plan de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le debe efectuar ajustes para su funcionalidad.

Los siguientes son los objetivos de control de las pruebas del plan:

a. Validar la habilidad de los responsables y la consistencia de los procedimientos en eventos de recuperación de siniestros.
b. Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados
c. Identificar y corregir falla en el Plan de Contingencias de TI
d. Facilitar la divulgación y el entrenamiento en los procedimientos de recuperación.
e. Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias.
f. Motivar a los encargados involucrados en el diseño y desarrollo del Plan a mantener actualizados los procedimientos inherentes.

10.2. **Cronograma de Pruebas**

N°	EVENTO	I SEMESTRE 2019	II SEMESTRE 2019
1	Caída o interrupción de energía eléctrica	X	
2	Infección masiva por software malicioso	X	
3	Suspensión de las actividades por sismo o incendio	X	
4	Falla técnica en servidores		X
5	Falla en Sistemas de Información críticos		X
6	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes		X
7	Calentamiento del Centro de Datos		X

XI. PRESUPUESTO PARA LA EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

11.1. El Plan de Contingencia de Tecnologías de la Información contiene actividades que serán desarrolladas por el personal de la Unidad de Tecnologías de la Información, de acuerdo a sus competencias, las cuales no ameritan contar con un presupuesto específico para la ejecución de las mismas.

XII. SEGUIMIENTO Y MEJORA CONTINUA

12.1. El responsable del mantenimiento y mejora continua del plan es el Oficial de Seguridad de la Información. El plan debe ser revisado, probado y actualizado en su documentación y su alcance, esto quiere decir que el plan debe tener revisiones de acuerdo a los siguientes parámetros:

- Implementación de nuevos servicios críticos de TI
- Resultados de una nueva evaluación de riesgos.
- Requisitos legales o contractuales.

PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA
VºBº
JEFA DE LA UNIDAD DE TEC DE LA INFORMACIÓN

V°B°
UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN
B. MORALES F.

Formato de registro de Contingencia

Warma	PLAN DE CONTINGENCIA DE TI	Codigo Documento PNAEQW-UTI-PCTI-01 Version 1.0

REGISTRO DE CONTINGENCIA

Orden	Fecha activación	Hora activación	Unidad que informa la contingencia	Personal que informa la contingencias	Descripcion de contingencia	Hora finalización de la activación	Firma de quien autoriza la activación	Pruebas realizadas	Firma de quien autoriza el cierre de la activación

Formato de registro del Plan de Pruebas

QaliWarma	**PRUEBAS PLAN DE CONTINGENCIA DE TI**	Codigo Documento PNAEQW-UTI-PRB-01 Version 1.0

Fecha:	**Hora:**	**Lugar:**

Nombre de Prueba:

INFORMACION DE RECUPERACION

ACTIVIDADES DESARROLLADAS	PERSONAL PARTICIPANTE	RESULTADO ESPERADO	RESULTADO OBTENIDO	TIEMPO INVERTIDO	OBSERVACIONES