

Decenio de la Igualdad de Oportunidades para mujeres y hombres
"Año de la Lucha contra la Corrupción y la Impunidad"



RESOLUCION DIRECTORAL

San Borja, 01 FEB. 2019

VISTO:

El Expediente Nº 18-025231-001 sobre la elaboración del proyecto del "Plan de Contingencia de TI" del Instituto Nacional de Salud del Niño San Borja, y;

CONSIDERANDO:

Que, el Instituto Nacional de Salud del Niño-San Borja es un órgano desconcentrado especializado del Ministerio de Salud - MINSA, que según Manual de Operaciones, aprobado mediante Resolución Ministerial Nº 512-2014/MINSA y modificado mediante Resolución Directoral Nº 123-2017/INSN-SB, tiene como misión brindar atención altamente especializada en cirugía neonatal compleja, cardiología y cirugía cardiovascular, neurocirugía, atención integral al paciente quemado y trasplante de médula ósea y, simultáneamente realiza investigación y docencia, proponiendo el marco normativo de la atención sanitaria compleja a nivel nacional;

Que, el artículo 2º de la Ley que Establece la Obligación de Elaborar y Presentar Planes de Contingencia - Ley Nº 28551, define los planes de contingencia como instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos;

Que, el artículo 3º del mismo cuerpo normativo, prescribe que todas las personas naturales y jurídicas de derecho privado o público que conducen o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle;

Que, el literal b) del artículo 6º de la Ley de Control Interno de las Entidades del Estado - Ley Nº 28716, prescribe que son obligaciones del Titular y funcionarios de la entidad, relativas a la implantación y funcionamiento del control interno organizar, mantener y perfeccionar el sistema y las medidas de control interno, verificando la efectividad y oportunidad de la aplicación, en armonía con sus objetivos, así como efectuar la autoevaluación del control interno, a fin de propender al mantenimiento y mejora continua del control interno;

Que, mediante Resolución de Contraloría Nº 320-2006-CG, la Contraloría General de la República resuelve aprobar las Normas de Control Interno, que son de aplicación a las Entidades del Estado, de conformidad con lo establecido por la Ley de Control Interno de las

Entidades del Estado – Ley N° 28716. Al respecto, su numeral 3.10 establece los controles para las Tecnologías de la Información y Comunicaciones y precisa que la información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir erros e irregularidades mientras la información fluye a través de los sistemas;

Que, el numeral II.3.5 del Manual de Operaciones del Instituto Nacional de Salud del Niño San Borja establece que la Unidad de Tecnologías de la Información es la unidad de apoyo del INSN-SB encargada de la gestión de la información en el Instituto, mediante tecnologías de la información y comunicaciones, así como de la información epidemiológica y sanitaria en virtud del Sistema Nacional de Vigilancia en Salud Pública;

Que, mediante Nota Informativa N° 0653-2018-UTI-INSNSB, el Director Ejecutivo de la Unidad de Tecnologías de la Información remite al Director Ejecutivo de la Unidad de Planeamiento y Presupuesto, el proyecto del "Plan de Contingencia de TI" elaborado por la Coordinación Técnica de Informática, conforme a lo expuesto en la Nota Informativa N° 0105-2018-INF-UTI-INSNSB, cuyo objetivo es garantizar la continuidad en la prestación de los servicios al Ciudadano en el Instituto Nacional de Salud del Niño San Borja, ante eventos que puedan afectar el normal funcionamiento de los Sistemas de Información y Comunicaciones que afecten a procesos críticos de la Institución, restableciendo los servicios en el menor tiempo posible a través de la ejecución de procedimientos, contratos, coordinaciones y acciones que permitan enfrentar las contingencias. En tal sentido, solicita la revisión y correspondiente opinión técnica y, de ser favorable, su recomendación para la aprobación mediante acto resolutivo;

Que, mediante Informe N° 086-2018-UPP/INSNSB, el Director Ejecutivo de la Unidad de Planeamiento y Presupuesto informa a la Jefa de Oficina de la Unidad de Asesoría Jurídica de la opinión favorable por parte de su Despacho, respecto al proyecto del "Plan de Contingencia de TI", elaborado por la Coordinación Técnica de Informática de la Unidad de Tecnologías de la Información; concluyendo que el proyecto del "Plan de Contingencia de TI" se encuentra articulado con los objetivos institucionales y Plan Operativo Institucional 2018 y recomienda continuar con el trámite para su aprobación;

Que, mediante Informe Legal N° 021-2019-UAJ-INSN-SB, la Jefa (e) de Oficina de la Unidad de Asesoría Jurídica informa a la Dirección General de la opinión favorable de su Despacho, respecto al proyecto del "Plan de Contingencia de TI", elaborado por la Coordinación Técnica de Informática de la Unidad de Tecnologías de la Información, toda vez que él mismo es concordante con el marco normativo vinculado a la materia;

Que, el Manual de Operaciones del Instituto Nacional de Salud del Niño San Borja, establece en su numeral II.2.1. que la Dirección General es la máxima autoridad del INSN-SB y está a cargo de la conducción general, coordinación y evaluación de los objetivos, políticas, proyectos, programas y actividades que corresponden al Instituto Nacional de Salud del Niño San Borja;

Con el visto bueno del Director Adjunto, del Director Ejecutivo de la Unidad de Planeamiento y Presupuesto, del Director Ejecutivo de la Unidad de Tecnologías de la Información y, de la Jefa (e) de Oficina de la Unidad de Asesoría Jurídica;

Estando a lo dispuesto en la Ley N° 28551, en la Ley N° 28716, en el TUO de la Ley de Procedimiento Administrativo – Ley N° 27444, aprobado mediante el Decreto Supremo N° 004-2019, en la Resolución de Contraloría N° 320-2006-CG, en la Resolución Ministerial N° 512-2014/MINSA, en la Resolución Directoral N° 123-2017/INSN-SB y, en la Resolución Ministerial N° 021-2019/MINSA;

SE RESUELVE:

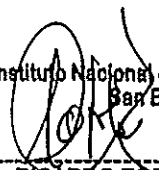

ARTÍCULO 1°.- APROBAR el "Plan de Contingencia de TI" del Instituto Nacional de Salud del Niño San Borja, elaborado por la Coordinación Técnica de Informática de la Unidad de Tecnologías de la Información, que como anexo adjunto forma parte del presente acto resolutivo.

ARTÍCULO 2°.- DISPONER que la Unidad de Tecnologías de la Información informe a la Dirección General, sobre los resultados alcanzados con el desarrollo del "Plan de Contingencia de TI" del Instituto Nacional de Salud del Niño San Borja.

ARTÍCULO 3°.- DISPONER la publicación de la presente Resolución en la Página Web de la Entidad, conforme a las normas de Transparencia y Acceso a la Información Pública.



REGÍSTRESE, COMUNÍQUESE Y PUBLÍQUESE


insn  Instituto Nacional de Salud del Niño
San Borja
Dr. A. RICARDO ZORFI RUBIO
Director General (e)
CMP. 8780 RNE. 2550

ARZR/JELC
CC.
DA
UPP
UTI
UAI
Archivo



PERÚ

Ministerio
de Salud

Instituto Nacional de Salud
del Niño San Borja



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

PLAN DE CONTINGENCIAS DE TI

INSTITUTO NACIONAL DE SALUD DEL NIÑO SAN BORJA

UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN



2018



INDICE

1. INTRODUCCIÓN	3
2. OBJETIVO	3
3. ALCANCE	4
4. BASE LEGAL	4
5. ESTRUCTURA DEL PLAN DE CONTINGENCIAS	5
5.1. Organización de roles y responsabilidades	5
5.2. Identificación y priorización de riesgos	8
5.3. Análisis y clasificación de los riesgos	12
5.4. Inventario de equipos y sistemas de información	22
5.5. Actividades del plan según el riesgo	25
5.6. Procedimiento del Plan de Contingencias de TI	38
5.7. Plan de Pruebas	41
5.8. Actualización del Plan	43
6. VARIABLES TÉCNICAS A TENER EN CUENTA EN LA IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIAS DE TI	43
7. RECOMENDACIONES	44
8. ANEXOS	45





1. INTRODUCCIÓN

Desde su creación el Instituto Nacional de Salud del Niño de San Borja brinda atención Especializada Quirúrgica Compleja contando con procesos administrativos y asistenciales que se apoyan en las Tecnologías de la Información y Comunicaciones. La Unidad de Tecnologías de la Información es la encargada velar por la disponibilidad, continuidad, respaldo y seguridad del software, hardware e información necesarios para brindar los servicios al ciudadano. La respuesta ante cualquier riesgo sobre los sistemas de información y comunicaciones que afecten la prestación de servicios al ciudadano es responsabilidad de la Unidad de Tecnología de la Información, por lo que en el presente Plan de Contingencias se indicarán las acciones a realizar para mantener o reestablecer los servicios en el menor tiempo posible bajo el contexto de los recursos Tecnológicos y Humanos con los que se cuenta en la actualidad.

2. OBJETIVO

2.1. General

Garantizar la continuidad en la prestación de servicios al Ciudadano en el Instituto Nacional de Salud del Niño de San Borja ante eventos que puedan afectar el normal funcionamiento de los Sistemas de Información y Comunicaciones que afecten a procesos críticos de la Institución, restableciendo los servicios en el menor tiempo posible a través de la ejecución de procedimientos, contratos, coordinaciones y acciones que permitan enfrentar las contingencias.

2.2. Específicos

- Identificar y mitigar los riesgos a los que se encuentran expuestos los Sistemas de Información y Comunicaciones del INSNSB.
- Minimizar las consecuencias en caso de pérdida de información relacionada con eventos inesperados a un nivel aceptable, mediante la realización de procedimientos de respaldo y recuperación adecuados.
- Mantener la continuidad en la prestación de servicios al ciudadano.
- Restablecer el funcionamiento de los Sistemas de Información y Comunicaciones del INSNSB en el menor tiempo posible de acuerdo al grado de afectación que produzca el evento inesperado.
- Mantener operativos los sistemas de información y Comunicaciones que apoyen procesos críticos de la Institución ante eventos que afecten parcial o totalmente las instalaciones, cableado, equipos, sistemas de información con los que cuenta el INSNSB para este fin.





- Minimizar la posible pérdida económica, operativa y afectación de la imagen institucional ante eventos que afecten la disponibilidad de los Sistemas de Información y Comunicaciones.

3. ALCANCE

El Presente Plan de Contingencias de TI de Instituto Nacional de Salud del Niño de San Borja abarca a la infraestructura (Data Center, Cuartos de Comunicaciones, Cableado, Suministro Eléctrico), Hardware, Software, Equipos de comunicaciones y Sistemas de Información que apoyan a los procesos críticos del INSNSB como son SIGA, SIAF, SISGALENPLUS, Bases de Datos y Documentos Institucionales Digitalizados.

4. BASE LEGAL

- Ley N° 28551, Ley que Establece la Obligación de Elaborar y Presentar Planes de Contingencia
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)
- Decreto Supremo N° 048-2011-PCM, Reglamento de la Ley N° 29664, que crea el Sistema Nacional del Riesgo de Desastres (SINAGERD)
- Decreto Supremo N° 111-2012-PCM, que incorpora la Política Nacional de Gestión de Riesgo de Desastres como Política Nacional de Obligatorio Cumplimiento para las Entidades del Gobierno Nacional
- Resolución Ministerial N° 517-20004/MINSA, que aprobó la Directiva N° 036-2004-OGDN/MINSA-V.01 "Declaratoria de Alertas en Situaciones de Emergencia y Desastres"
- Resolución Ministerial N° 768-20004/MINSA, que aprobó la Directiva N° 040-2004-OGDN/MINSA-V.01 "Procedimiento para la elaboración de Planes de Contingencia para Emergencias y Desastres"
- Resolución Ministerial N° 974-20004/MINSA, que aprobó la Directiva N° 043-2004-OGDN/MINSA-V.01 "Procedimiento para la elaboración de Planes de Respuesta frente a Emergencias y Desastres"
- Resolución Ministerial N° 114-2017/MINSA, que aprobó el Plan de Contingencias del Ministerio de Salud, frente a los efectos de las lluvias 2017-2018.
- Resolución Jefatural N° 386-2002-INEI, que aprobó la Directiva N° 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de Información procesada por las Entidades de la Administración Pública".
- Resolución Jefatural N° 347-2001-INEI, que aprobó la Directiva N° 018-2001-INEI/DTNP "Normas y Procedimientos Técnicos para Garantizar la Seguridad de la Información Publicada por las Entidades de la Administración Pública".





5. ESTRUCTURA DEL PLAN DE CONTINGENCIAS

- Organización roles y responsabilidades.
- Identificación y priorización de los riesgos.
- Análisis y clasificación de los riesgos.
- Inventario de hardware, software y Sistemas de Información
- Actividades del plan según el riesgo.
- Procedimiento del Plan de Contingencias de TI
- Prueba del Plan de Contingencias de TI
- Actualización del Plan de Contingencias de TI

5.1. Organización de roles y responsabilidades

5.1.1. Comité de Contingencia de Tecnología de la Información

El Comité de Contingencia de Tecnología de la Información es el órgano donde se coordinan y aprueban todas las actividades que se ejecutarán en caso de algún evento que afecte la continuidad de los Sistemas de Información y Comunicaciones que apoyan a los procesos críticos de la institución.

Este comité se reunirá por lo menos con una periodicidad semestral para definir los lineamientos del Plan de Contingencias

Integrantes:

- a) Director(a) General del INSNSB o su representante (Presidente)
- b) Director(a) de la Unidad de Tecnologías de la Información (Coordinador).
- c) Director(a) de la Unidad de Atención Integral Especializada o su representante
- d) Director(a) de la Unidad de Planeamiento y Presupuesto
- e) Director(a) de la Unidad de Administración o su representante
- f) Jefe de la Oficina de Comunicaciones.
- g) Jefe de la Oficina Asesora Jurídica.

El Director(a) General, Director(a) Médico y Director(a) de Administración, designará a otros integrantes que considere pertinente a participar en el comité.





Funciones y Roles del Comité de Contingencia T.I

- Participar en las reuniones periódicas propuestas por el Coordinador del Plan de Contingencias.
- Proponer, aprobar o rechazar la incorporación y/o modificaciones del Plan de Contingencias Informático.
- Coordinar, ejecutar y verificar que el personal se encuentre debidamente capacitado en la ejecución del Plan de Contingencias.
- Coordinar la ejecución de las actividades del plan de pruebas.
- Aprobar los informes presentados por la coordinación del plan.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.
- Realizar las coordinaciones para contar con la disponibilidad de recursos y/o servicios necesarios para soportar la operativa y restauración los servicios afectados por algún evento imprevisto.

5.1.2. Coordinador del Plan de Contingencias de Tecnología de la Información

El Coordinador del Plan es el canal de comunicación entre el Equipo de Desarrollo del Plan de Contingencias y el Comité de Contingencia T.I. a través del cual se transmitirán las decisiones tomadas referidas a las acciones del Plan de Contingencias Informático, los niveles de ejecución del Plan y el estado de los recursos informáticos y de comunicaciones que se encuentran en el alcance del Plan. Es el que autoriza la puesta en marcha del Plan de Contingencias cuando lo considere necesario de acuerdo con el reporte dado por el Grupo de Desarrollo del Plan.

El Coordinador del Plan de Contingencias de T.I. es el Director(a) de la Unidad de Tecnología de la Información del INSNSB o quien haga sus veces y en su ausencia el Ingeniero que delegue.

Funciones:

- Proponer políticas y acciones para el Plan de Contingencias TI
- Mantener actualizado el Plan de Contingencias de TI.
- Autorizar la ejecución del Plan de Contingencias de TI.
- Elaborar los informes referidos al Plan.
- Proponer reuniones para revisión del Plan de Contingencias de TI.
- Encargado de monitorear y asegurar el cumplimiento del Plan.
- Mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo.





5.1.3. Equipo de Desarrollo del Plan

Está constituido por los colaboradores responsables de la ejecución de las tareas definidas dentro del plan. El grupo estará conformado por:

- a) Coordinador Técnico de Informática
- b) Coordinador de Plataforma Informática
- c) Administrador de Base de Datos
- d) Coordinador de Desarrollo
- e) Especialistas en Desarrollo
- f) Coordinador de Soporte Informático
- g) Técnicos en Soporte Informático
- h) Un Usuario Funcional de los Sistemas SIGA y SIAF
- i) Un Usuario Funcional de Admisión
- j) Un Usuario Funcional de Módulos Asistenciales (Consultorios Externos y Hospitalización)

Funciones:

- Ejecutar las actividades del Plan de Contingencias de T.I.
- Documentar el Plan de Contingencias de T.I.
- Ordenar la documentación y registros de trabajo durante la contingencia.
- Diseñar planes de capacitación para los colaboradores de la entidad que actuarán durante la contingencia.
- Realizar las pruebas necesarias al Plan de Contingencias de T.I.

5.1.4. Equipo de Seguimiento y Control

Conformado por los representantes de la Oficina de Control Interno, están encargados del seguimiento y control de las labores que se ejecuten, velando por la viabilidad y el cumplimiento en la aplicación del plan.

Funciones:

- Verificar que el Plan de Contingencias se encuentre actualizado.
- Revisar y verificar que Plan de Contingencias se enmarque dentro del alcance establecido.
- Velar por la disponibilidad de los recursos necesarios para viabilizar el Plan de Contingencias.
- Verificar que el Plan de Contingencias se cumpla correctamente.





- Presentar los informes del Plan de Contingencias al Comité de Contingencia de T.I.
- Certificar que todos los recursos descritos en el Plan de Contingencias (infraestructura, software, hardware, humanos, bienes, servicios, etc.) sean viables y se encuentren disponibles para su uso ante un evento inesperado.
- Auditar los procesos que forman parte del Plan de Contingencias de T.I. corroborando que se cumpla correctamente.
- Participar y visar las pruebas del Plan de Contingencias.
- Informar al Comité respecto a cualquier evento o anomalía encontrada que ponga en riesgo la ejecución de todo o parte del plan.
- Proponer y recomendar actividades o procesos de mejora.

5.2. Identificación y priorización de riesgos

5.2.1. Definiciones

5.2.1.1. Riesgo

Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la prestación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.

5.2.1.2. Amenaza

Posible peligro que una situación, un objeto o una circunstancia específica puede conllevar para la vida, de uno mismo o de terceros o de un sistema. Es un peligro que está latente, que todavía no se ha desencadenado pero que sirve como aviso para prevenir o para presentar la posibilidad de que sí lo haga. Posibilidad de ocurrencia de un suceso.

5.2.1.3. Vulnerabilidad

Nivel susceptibilidad a sufrir un daño o pérdida por la ocurrencia de un peligro o amenaza.

5.2.1.4. Plan de Contingencias

Plan que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad o procesos para la prestación de servicios al ciudadano.





5.2.2. Descripción de los Riesgos Externos

5.2.2.1. Incumplimiento contractual de Bienes y Servicios. - (R1)

Riesgo externo que consiste en el atraso que puede presentar la ejecución o incumplimiento de la adquisición de bienes o servicios de actualización, modificación, mantenimiento y soporte del hardware, software, insumos y servicios de custodia de copias de respaldo, Data Center alternativo y conexión a internet que afecten a los sistemas de información catalogados como críticos (SIGA, SIAF, SISGALENPLUS, Bases de Datos y Documentos Institucionales Digitalizados) que al presentarse genera inoperancia de los sistemas de información o mala imagen de la entidad. Tipo de riesgo: Cumplimiento.

5.2.2.2. Caída o interrupción del sistema eléctrico - (R2)

Riesgo externo. Corresponde al corte del servicio de energía eléctrica en el INSNSB por falla externa del proveedor del servicio, que genera la interrupción del funcionamiento de los equipos donde se alojan o ejecutan los sistemas de información críticos de la entidad y que afectan directamente la prestación de servicios al ciudadano. Tipo de riesgo: Tecnológico.

5.2.2.3. Caída de Conexión a internet - (R3)

Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet en INSNSB, lo que ocasionaría suspensión de los servicios de Verificación de Cobertura de Pacientes Asegurados, Verificación de Identidad, Actualización de Catálogos SIGA, Transmisiones SIAF, Web Services de Integración con entidades Externas y Correo electrónico. Tipo de riesgo: Tecnológico.

5.2.2.4. Caída del Servicio Telefónico - (R4)

Riesgo externo. Originado por la suspensión del servicio por falta de pago, daños o fallas en el operador de Telecomunicaciones, en el software o hardware de telefonía en el INSNSB, que de presentarse genera la ausencia de comunicación telefónica en la entidad. Tipo de riesgo: Tecnológico.

5.2.2.5. Ataque de Malware / Virus Informáticos - (R5)

Riesgo externo. Es el riesgo de infección de los equipos de cómputo y servidores que puede presentarse en la entidad por problemas o fallas en la actualización de los sistemas operativos, plataforma antivirus o por ausencia de políticas de seguridad, ocasionando la suspensión total o parcial el funcionamiento o prestación de los servicios de red, acceso a





la información, acceso o inestabilidad de los sistemas de información críticos. Tipo de riesgo: Tecnológico.

5.2.2.6. Suspensión del servicio por sismo, inundación o incendio - (R6)

Riesgo externo. Hace referencia al riesgo que corre la entidad ante un sismo, inundación o incendio que afecte la infraestructura tecnológica (Data Center, redes, servidores, switches, computadoras, conexiones eléctricas) que soportan a los sistemas de información críticos de la institución ocasionando la suspensión total o parcial en el funcionamiento de los sistemas o inestabilidad de los mismos. Tipo de riesgo: Operativo.

5.2.3. Descripción de los Riesgos Internos

5.2.3.1. Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y Comunicaciones. - (R7)

Riesgo interno que corresponde a retrasos en los procesos de adquisición de bienes o servicios relacionados con los Sistemas de Información y Comunicaciones de la Institución por deficiente planificación del proceso de contratación, fallas o incumplimiento de plazos para realizar los estudios previos de contratación. Esto puede ocasionar Inoperancia de los sistemas de información y respaldo de información, debido a falta de recursos, servicios y desactualización de los sistemas de información. Tipo de riesgo: Operativo

5.2.3.2. Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles - (R8)

Riesgo interno que se relaciona con deficientes procesos de análisis, evaluación, planificación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas y con el probable desconocimiento de las características y especificaciones técnicas de los recursos disponibles y necesarios en cada una de las soluciones elegidas. Al materializarse el riesgo la infraestructura tecnológica puede generar inoperancia de los sistemas de información. Tipo de riesgo: Operativo.

5.2.3.3. Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción. - (R9)

Riesgo interno que tiene baja probabilidad de ocurrencia y consiste en el robo, alteración o extracción de la información que es considerada confidencial o clasificada como reservada por deficiencia en las políticas





de seguridad o Configuración ineficiente del corta fuegos de la entidad. Al materializarse, el impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional. Tipo de riesgo: Tecnología.

5.2.3.4. Falla técnica en Servidores, equipos de escritorio o de comunicaciones. - (R10)

Riesgo interno que corresponde al daño físico o lógico de un Servidor, computadoras de escritorio o equipos de comunicaciones que afectan 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 usuarios, ocasionando que el servicio quede inoperativo o inestable. Tipo de riesgo: Tecnológico.

5.2.3.5. Falla técnica en sistemas de información - (R11)

Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación, actualizaciones con errores o incompatibilidad entre software que afectan a los sistemas de información que genera inoperatividad o inestabilidad de los sistemas de información. Tipo de riesgo: Tecnológico.

5.2.3.6. Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información. - (R12)

Riesgo interno. Corresponde a la falta o inasistencia en un momento dado, de un ingeniero o técnico de la Unidad de Tecnología de la Información que realiza actividades de soporte a usuarios o de administración de un sistema de información crítico de la Institución por enfermedad, muerte o incapacidad de los colaboradores o demoras en la contratación o asignación de colaboradores para la Unidad de Tecnologías de la Información, lo que genera inoperatividad o inestabilidad de los sistemas de información. Tipo de Riesgo: Operativo.



5.2.3.7. Mal uso de hardware y/o software por parte de los colaboradores del INSNSB - (R13)

Riesgo interno. Consiste en el riesgo por un uso inadecuado de los equipos de cómputo, software y/o sistemas de información por parte de los colaboradores por deficiencias en el conocimiento y uso de las herramientas tecnológicas o por uso mal intencionado de los mismos, lo que puede ocasionar la interrupción del funcionamiento de los equipos informáticos y de comunicaciones que soportan a los sistemas de



información críticos de la Institución, pudiendo dejar los servicios y aplicativos inoperativos. Tipo de riesgo: Tecnología.

5.2.3.8. Calentamiento del centro de cómputo - (R14)

Riesgo interno que consiste en el aumento de temperatura dentro del centro de cómputo, 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 servidores y equipos de comunicaciones dejándolos inoperativos junto con los servicios que se encuentran soportados por ellos. Tipo de riesgo: Tecnología

5.3. Análisis y clasificación de los riesgos

5.3.1. La Calificación del Riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se puede presentar en un determinado tiempo y la segunda se refiere a la magnitud de sus efectos.

5.3.2. Probabilidad

Posibilidad de ocurrencia del riesgo. Se puede medir con criterios de Frecuencia y Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

Probabilidad	Descripción	Frecuencia	Valor
Frecuente	El evento probablemente ocurrirá en la mayoría de los casos	Más de una vez al año	4
Probable	El evento probablemente ocurrirá en la mayoría de los casos	Al menos una vez en el último año	3
Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años	2
Improbable	El evento podría ocurrir en algún momento	Al menos una vez en los últimos cinco años.	1



**5.3.3. Impacto**

Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Impacto	Descripción	Valor
Catastrófico	<p>Si el hecho llegara a presentarse, tendría consecuencias o efectos desastrosos sobre la institución:</p> <ul style="list-style-type: none"> - Pérdida de recursos críticos. - Interrupción total o disminución considerable del rendimiento de los procesos de negocio. - Inoperatividad de los sistemas de información y comunicaciones críticos. - Pérdida de información confidencial estratégica. - Deterioro de la imagen institucional. 	4
Moderado Impacto	<p>Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la institución.</p> <ul style="list-style-type: none"> - Pérdida de recursos críticos que cuentan con respaldo o contingencia. - Interrupción parcial o disminución moderada del rendimiento de los procesos de negocio y los sistemas de información que los soportan. - Pérdida de información confidencial estratégica. 	3
Bajo Impacto	<p>Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución.</p> <ul style="list-style-type: none"> - Pérdida de recursos no críticos que cuentan con respaldo o contingencia. - Interrupción o disminución temporal del rendimiento de los procesos de negocio y los sistemas de información que los soportan. - Pérdida de información interna no publicada. 	2
Insignificante	<ul style="list-style-type: none"> - Si el hecho llegará a presentarse tendría consecuencias o efectos mínimos sobre la Entidad: - Caída poco perceptible del rendimiento de los procesos y sistemas de información que los soportan. - Suspensión temporal del servicio. 	1

**5.3.4. La Evaluación del Riesgo**

Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos EXTREMOS, ALTOS, MODERADOS, BAJOS y fijar las prioridades de las acciones requeridas para su tratamiento.



PERÚ

Ministerio
de SaludInstituto Nacional de Salud
del Niño San Borja

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

(R): Corresponde al número del riesgo dentro de las matrices de análisis y evaluación de los riesgos.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

PROBABILIDAD	IMPACTO			
	Insignificante (1)	Bajo (2)	Moderado (3)	Catastrófico (4)
Frecuente (4)	M	A		
Probable (3)		M		
Posible (2)		M	M	A
Improbable (1)				M

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgos extrema: Reducir el riesgo, evitar, compartir o transferir

Zona de riesgo	Probabilidad * impacto (combinaciones PROB-IMPAC)	Tratamiento
	(3,4)-(4,3)-(4,5)	Reducir el riesgo, evitar, compartir o transferir
Alta	(2,4)-(3,3)-(4,2)	Reducir el riesgo, evitar, compartir o transferir
Moderada	(1,4)-(2,2)-(2,3)-(3,2)-(4,1)	Asumir el riesgo, reducir el riesgo
Baja	(1,1)-(1,2)-(1,3)-(2,1)-(3,1)	Asumir el riesgo



Los riesgos que se tendrán en cuenta en este Plan de Contingencias de TI son los catalogados como EXTREMOS, MODERADOS Y ALTOS, es decir aquellos que afectan en forma drástica la imagen institucional, la pérdida de información confidencial estratégica, la suspensión parcial o total del funcionamiento del hardware, software y/o sistemas de información del INSNSB considerados como críticos; esta valoración se da en términos de las consecuencias que acarrearía dicha suspensión.



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal del hardware, software y/o los sistemas de información de la entidad, son:

Tipo de Riesgo	Nº	Riesgo	Probabilidad	Impacto	Zona de Riesgo (Calificación)
Externo	1	Incumplimiento contractual de Bienes y Servicios	2	4	ALTA
Externo	2	Caída o interrupción del sistema eléctrico	4	3	EXTREMA
Externo	3	Caída de Conexión a internet	2	2	MODERADA
Externo	4	Caída del Servicio Telefónico	2	1	BAJA
Externo	5	Ataque de Malware / Virus Informáticos	2	4	ALTA
Externo	6	Suspensión del servicio por sismo, inundación o incendio	2	4	ALTA
Interno	7	Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y Comunicaciones	2	2	MODERADA
Interno	8	Contratación sin asistencia técnica, de Soluciones de Software no compatibles frente a los Requerimientos y Recursos Disponibles	2	2	MODERADA
Interno	9	Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción	3	4	EXTREMA
Interno	10	Falla técnica en Servidores, equipos de escritorio o de comunicaciones.	3	3	ALTA
Interno	11	Falla técnica en sistemas de información	2	2	MODERADA
Interno	12	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información.	3	3	ALTA
Interno	13	Mal uso de hardware y/o software por parte de los colaboradores del INSNSB	2	2	MODERADA
Interno	14	Calentamiento del centro de cómputo	3	3	ALTA





"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

De los riesgos identificados serán desarrollados los siguientes cuya calificación de riesgo es Extrema, Moderada o Alta.

Tipo de Riesgo	Nº	Riesgo	Probabilidad	Impacto	Zona de Riesgo (Calificación)
Externo	1	Incumplimiento contractual de Bienes y Servicios	2	4	ALTA
Externo	2	Caída o interrupción del sistema eléctrico	4	3	EXTREMA
Externo	3	Caída de Conexión a internet	2	2	MODERADA
Externo	5	Ataque de Malware / Virus Informáticos	2	4	ALTA
Externo	6	Suspensión del servicio por sismo, inundación o incendio	2	4	ALTA
Interno	7	Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y Comunicaciones	2	2	MODERADA
Interno	8	Contratación sin asistencia técnica, de Soluciones de Software no compatibles frente a los Requerimientos y Recursos Disponibles	2	2	MODERADA
Interno	9	Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción	3	4	EXTREMA
Interno	10	Falla técnica en Servidores, equipos de escritorio o de comunicaciones.	3	3	ALTA
Interno	11	Falla técnica en sistemas de información	2	2	MODERADA
Interno	12	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información.	3	3	ALTA
Interno	13	Mal uso de hardware y/o software por parte de los colaboradores del INSNSB	2	2	MODERADA
Interno	14	Calentamiento del centro de cómputo	3	3	ALTA



**5.3.5. Aplicación de Controles**

Una vez definidos los riesgos a los que se encuentra expuesta la entidad, aplicamos los controles que se tienen para disminuir el impacto de los mismos.

Para cada riesgo se efectúa un análisis de que controles preventivos o correctivos tiene la Unidad de Tecnología de la Información y se aplica el Procedimiento para elaborar y realizar monitoreo y seguimiento al mapa de riesgos institucional - Criterios para evaluar los controles).

CRITERIOS PARA EVALUAR LOS CONTROLES

CRITERIOS	PUNTAJE
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15
¿Está(n) definido(s) el(los) responsables(s) de la ejecución del control y del seguimiento?	5
¿El control es automático?	15
¿El control es manual?	10
¿La frecuencia de ejecución del control y seguimiento es adecuada?	15
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30
TOTAL	100

**ANÁLISIS DE VALORACIÓN DE LOS CONTROLES**

RANGO DE CALIFICACION DE LOS CONTROLES	PUNTAJE A DISMINUIR EN PROBABILIDAD
De 0 a 50	0
De 51 a 80	1
De 81 a 100	2



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

Los controles pueden hacer que un riesgo cambie su zona de clasificación, lo anterior teniendo en cuenta la Tabla ANÁLISIS DE VALORACIÓN DE LOS CONTROLES

Tipo de Riesgo	Nº	Riesgo	CALIFICACIÓN			Puntaje Final
			Probabilidad	Impacto	Controles	
Externo	1	Incumplimiento contractual de Bienes y Servicios	2	4	Pólizas de seguro de cumplimiento	15
Externo	2	Caída o interrupción del sistema eléctrico	4	3	Sistema de suministro de energía alterno	65
Externo	3	Caída de Conexión a internet	2	2	Ruta alterna de acceso a internet	70
Externo	4	Caída del Servicio Telefónico	2	1	Procedimiento técnico de verificación del servicio	15
Externo	5	Ataque de Malware / Virus Informáticos	2	4	Sistema antivirus Copias de seguridad	70
Externo	6	Suspensión del servicio por sismo, inundación o incendio	2	4	Copias de seguridad	65
Interno	7	Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y Comunicaciones	2	2	Procedimiento de Monitoreo de Cumplimiento del PAC	15
Interno	8	Contratación sin asistencia técnica, de Soluciones de Software no compatibles frente a los Requerimientos y Recursos Disponibles	2	2	Procedimiento de Adquisición de Bienes y Servicios Tecnológicos	15





"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

Interno	9	Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción	3	4	Equipo Cortafuegos Sistema antivirus en todos los equipos de cómputo y servidores Sistema de almacenamiento masivo SAN	70
Interno	10	Falla técnica en Servidores, equipos de escritorio o de comunicaciones.	3	3	Mantenimiento preventivo y correctivo de los equipos. Garantía de equipos y servidores vigente. Sistema de almacenamiento de Copias de seguridad	65
Interno	11	Falla técnica en sistemas de información	2	2	Copia de respaldo de las bases de datos y aplicaciones	65
Interno	12	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información.	3	3	Manuales técnicos de los aplicativos críticos entre ellos: SIGA, SIAF, SisGalenPlus, Bases de Datos, Documentos Digitalizados	15
Interno	13	Mal uso de hardware y/o software por parte de los colaboradores del INSNSB	2	2	Capacitaciones sobre el uso adecuado de las TIC's	30
Interno	14	Calentamiento del centro de cómputo	3	3	Sistema de Monitoreo de Data Center	30



Teniendo en cuenta las tablas de valoración de los controles y la tabla de desplazamiento, se tiene:



PERÚ

Ministerio
de SaludInstituto Nacional de Salud
del Niño San Borja

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

Tipo de Riesgo	Riesgo	Riesgo Inherente			Riesgo Residual		
		Probabilidad	Impacto	Calificación	Probabilidad	Impacto	Calificación
Externo	Incumplimiento contractual de Bienes y Servicios	2	4	ALTA	2	4	ALTA
Externo	Caída o interrupción del sistema eléctrico	4	3	ALTA	3	3	ALTA
Externo	Caída de Conexión a internet	2	2	MODERADA	1	2	BAJA
Externo	Caída del Servicio Telefónico	2	1	BAJA	2	1	BAJA
Externo	Ataque de Malware / Virus Informáticos	2	4	ALTA	1	4	MODERADA
Externo	Suspensión del servicio por sismo, inundación o incendio	2	4	ALTA	1	4	MODERADA
Interno	Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y	2	2	MODERADA	2	2	MODERADA





PERÚ

Ministerio
de SaludInstituto Nacional de Salud
del Niño San Borja

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

	Comunicaciones						
Interno	Contratación sin asistencia técnica, de Soluciones de Software no compatibles frente a los Requerimientos y Recursos Disponibles	2	2	MODERADA	2	2	MODERADA
Interno	Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción	3	4		2	4	ALTA
Interno	Falla técnica en Servidores, equipos de escritorio o de comunicaciones.	3	3	ALTA	2	3	MODERADA
Interno	Falla técnica en sistemas de información	2	2	MODERADA	1	2	BAJA
Interno	Ausencia de personal de la Unidad de Tecnologías de la Información que brindan	3	3	ALTA	3	3	ALTA





PERÚ

Ministerio
de SaludInstituto Nacional de Salud
del Niño San Borja

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

	soporte y mantenimiento a los sistemas de información.						
Interno	Mal uso de hardware y/o software por parte de los colaboradores del INSNSB	2	2	MODERADA	2	2	MODERADA
Interno	Calentamiento del centro de cómputo	3	3	ALTA	3	3	ALTA

5.4. Inventario de equipos y sistemas de información

A continuación se menciona la infraestructura tecnológica con que cuenta el Instituto Nacional de Salud del Niño San Borja, según Plan Operativo Informático 2018.



a) Hardware

Nº	HARDWARE	CANTIDAD
Servidores		
1	Servidores Blade	14
2	Servidores Rack	4
Computadoras personales		
3	Computadoras de Escritorio	558
4	Laptops	13
Impresoras		
5	Impresoras	300
Scanner		
6	Scanner	3
Otros		
7	Cámaras IP	303
8	Codecs Video Conferencia	2
9	Teléfonos IP	473

7



b) Software

Nº	SOFTWARE	CANTIDAD
Sistemas Operativos		
1	Windows 10	13
2	Windows 7	558
3	Windows Server 2008	12
4	Windows Server 2012	7
Motores de Base de Datos		
5	SQL Svr Enterprise 2012	2
6	SQL Svr Standard 2008	1
Antivirus		
7	GData End Point	675
Otros		
8	Sistemas propios	15

c) Conectividad

Nº	CONECTIVIDAD	CANTIDAD
Switches		
1	Switches	82
Wireless		
2	Wireless (Acces Point)	77
Otros		
3	UHF / VHF Vertex - Motorola CDR-500, Estación de radio VHF	1
4	Vertex VX-1700 E-NEX, Estación de radio UHF	1

d) Sistemas de información del INSNSB

En la siguiente tabla se listan los sistemas de información que tiene la entidad, sistemas que se encuentran en funcionamiento.

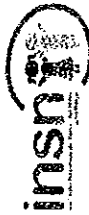
Los marcados con *asterisco (*)* se consideran críticos por su función de apoyo a los procesos de atención asistencial y administrativo para la prestación de servicios al paciente.





PERÚ
Ministerio
de Salud

Instituto Nacional de Salud
del Año del Seguro Social



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

Nombre del aplicativo informático, abreviatura		Descripción del Sistema		Usuarios		Tipo de Software		Tipo de Hardware	
1	SisGalenPlus *	Sistema de Gestión Hospitalaria que soporta la atención en admisión, caja, farmacia, consulta externa, emergencias y hospitalización.		Usuarios Administrativos y Asistenciales del INSNSB		Asistenciales		Visual Basic 6	
2	Sistema de Gestión de Documentos Alfreco	Sistema que permite administrar sitios web para compartir documentos dentro y fuera de la institución		Usuarios Administrativos y Asistenciales del INSNSB		Administrativos y Asistenciales		Java Web	
3	Sistema de Recursos Humanos	Sistema que permite el registro de personal, consulta de asistencia y gestión de contratos		Usuarios Administrativos		Administrativos		PHP	
4	Sistema de Convocatorias CAS	Sistema de soporte a los concursos CAS convocados por la institución		Usuarios Administrativos		Administrativos		PHP	
5	FISSAL	Sistema para el registro de prestaciones financiadas por FISSAL		Usuarios Administrativos		Administrativos		.NET	
6	Sistema de Directorio Telefónico	Sistema que permite administrar el directorio telefónico de la institución		Usuarios Administrativos y Asistenciales del INSNSB		Administrativos y Asistenciales		PHP	
7	Sistema de Trámite de Documentario *	Sistema de Gestión de Trámites Institucional		Usuarios Administrativos y Asistenciales del INSNSB		Administrativos y Asistenciales		ASP	
8	Sistema de Marcación de Asistencia	Sistema que permite la gestión de la asistencia del personal de la institución		Usuarios Administrativos y Asistenciales del INSNSB		Administrativos		Power Builder	
9	Sistema de Gestión de Aulas	Sistema que permite la separación de Aulas y salas de reuniones		Usuarios Administrativos, Asistenciales y Externos		Administrativos		PHP	
10	SIGA *	Sistema de Gestión Administrativa		Usuarios Administrativos y Asistenciales del INSNSB		Administrativos		Power Builder	
11	SIAP *	Sistema de Gestión Administrativo Financiera		Usuarios Administrativos		Administrativos		Visual Fox Pro	
12	Web Institucional	Página Web Institucional http://www.insnb.gob.pe		Usuarios Externos e Internos		Administrativos y Asistenciales		WordPress	
13	Web Docencia	Página Web http://www.insnb.gob.pe/docencia		Usuarios Externos e Internos		Administrativos y Asistenciales		WordPress	
14	Web Investigación	Página Web http://www.insnb.gob.pe/investigacion		Usuarios Externos e Internos		Administrativos y Asistenciales		WordPress	
15	Biblioteca Virtual	Biblioteca Virtual del INSNSB http://bibliotecavirtual.insnb.gob.pe		Usuarios Externos e Internos		Administrativos y Asistenciales		WordPress	
16	TeleSalud	Página Web http://telesalud.insnb.gob.pe		Usuarios Externos e Internos		Administrativos y Asistenciales		WordPress	
17	PCSISTEL	Sistema Tarifador y Control de llamadas		Usuarios Internos		Administrativos		.Net	
18	Tablero de Gestión	Página Web http://www.insnb.gob.pe/tablerodegestion		Usuarios Externos e Internos		Administrativos y Asistenciales		PHP, Reporting Services	
19	Sistema de llamado de Pacientes en consultorios Externos	Sistema para la visualización y llamado de pacientes en consultorios externos a través del sistema SIGALENPLUS		Usuarios Externos e Internos		Asistenciales		Android, MVC sobre Net	





5.5. Actividades del plan según el riesgo

Como se determinó anteriormente, los riesgos que se tienen en cuenta en este Plan de Contingencias de TI son los riesgos residuales calificados como EXTREMOS Y ALTOS.

5.5.1. R1-Incumplimiento contractual de Bienes y Servicios

Usuario: Todas las áreas del INSNSB

Descripción: El riesgo de incumplimiento contractual de Bienes y Servicios es ALTO debido al impacto que tiene sobre la disponibilidad de los Servidores y Equipos de Comunicaciones que soportan los procesos de atención a los Ciudadanos. Puede ocasionar pérdida de información, interrupción parcial de los servicios informáticos y/o suspensión de los servicios.

Protección:

- Contamos con mantenimientos preventivos programados.
- Revisiones periódicas de los registros de programación y ejecución de los mantenimientos programados.
- Contar con copias de seguridad actualizadas

En la contingencia:

1. Informar a la Unidad de Tecnologías de la Información sobre el problema presentado.
2. Apertura de Ticket reportando la incidencia a GEPEHO
3. Evaluar tiempo de solución del problema por parte de la GEPEHO
4. De ser necesario Gestionar el alquiler de equipos
5. Utilizar formatos manuales y archivos en Excel para el registro de la información correspondiente a los sistemas de información afectados para su posterior ingreso al sistema.



Después de la contingencia:

1. Cerrar Ticket o realizar Queja por incumplimiento.
Solicitar el ingreso de la información registrada en los archivos de Excel en el sistema de información correspondiente.



5.5.2. R2- Caída o interrupción del sistema eléctrico

Usuario: Todas las áreas del INSNSB

Descripción: El riesgo de la caída de los Sistemas de Información y Comunicaciones por interrupción del servicio eléctrico es ALTA debido al impacto que tiene sobre los procesos de atención al Ciudadano. Puede ocasionar pérdida de información; avería de Servidores, Switches, Computadoras, operativa parcial y/o suspensión de los servicios de T.I.

Protección:

- Contamos con 04 UPS de 40 KVA cada una con una autonomía total de 60 minutos para el Data Center, los Cuartos de Comunicaciones cuentan con UPS de 5 KVA con autonomía 10 minutos, para asegurar el suministro eléctrico de los servidores y equipos de comunicaciones.
- Contrato con GEPEHO que incluye el mantenimiento de los UPS.
- Revisiones periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Revisiones periódicas de los registros de programación y ejecución de los mantenimientos programados.
- Contar con copias de seguridad actualizadas

En la contingencia:

1. Informar a la Dirección de Tecnologías de la Información problema presentado.
2. Activación automática de los UPS.
3. Apertura de Ticket reportando la incidencia a GEPEHO
4. Monitorear el tiempo de autonomía de las UPS para no exceder el límite.
5. Gestionar el encendido del Grupo Electrónico
6. Monitorear la autonomía del Grupo Electrónico.
7. Si por algún motivo no se restablece el suministro eléctrico externo o no entra en funcionamiento el grupo electrónico por más de 40 minutos se procederá al apagado de los servidores hasta que regrese el servicio de energía.
8. En caso de haber apagado los servidores, se utilizarán los formatos manuales y archivos en Excel para el registro de la información correspondiente a los sistemas de información afectados para su posterior ingreso al sistema.

Después de la contingencia:

1. Contactar a Servicios Generales y GEPEHO para que informen la causa y medidas correctivas y preventivas para tratar este tipo de





problema.

2. Cerrar Ticket o realizar Queja por incumplimiento.
3. Solicitar el ingreso de la información registrada en los archivos de Excel en el sistema de información correspondiente.

5.5.3. R5 - Ataque de Malware / Virus Informáticos

Usuario: Todas las áreas del INSNSB

Descripción: El riesgo de Ataque de Malware o Virus Informáticos se considera MODERADO ya que pueden afectar a los Servidores y equipos de cómputo utilizados para dar servicio al ciudadano, ocasionando la interrupción parcial del servicio informático afectado.

Protección:

1. Plataforma de Firewall actualizada
2. Plataforma Endpoint (Antivirus) actualizada
3. Gestión de Actualizaciones de Sistemas Operativos
4. Copias de seguridad actualizadas

En la contingencia:

1. Informar a la Dirección de Tecnologías de la Información problema presentado.
2. Apagado de Equipo Afectado.
3. Escaneo en busca de Malware/Virus en simultáneo en todos los Equipos de la red del INSNSB
4. Habilitación de Equipo de Contingencia en caso de servidores o computadoras considerados como críticos.
5. En caso de haber afectado a los servidores o equipos de cómputo críticos, se utilizarán los formatos manuales y archivos en Excel para el registro de la información correspondiente a los sistemas de información afectados para su posterior ingreso al sistema.



Después de la contingencia:

1. Contactar a Servicios Generales y GEPEHO para que informen la causa y medidas correctivas y preventivas para tratar este tipo de problema.
2. Cerrar Ticket o realizar Queja por incumplimiento.
3. Solicitar el ingreso de la información registrada en los archivos de Excel en el sistema de información correspondiente.



5.5.4. R6 - Suspensión del servicio por sismo, inundación o incendio

POR SISMO

Usuario: Todas las áreas del INSNSB.

Descripción: Suspensión parcial del servicio por sismo. Este riesgo se considera MODERADO por la magnitud de pérdidas que ocasiona y la suspensión del servicio.

Protección:

- Anclaje de equipos de Informáticos.
- Plan de evacuación de las instalaciones del INSNSB.
- Realización de simulacros de evacuación con la participación de todos los colaboradores.
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas y pasillos.
- Señalizar las zonas seguras.
- Acatar las indicaciones de la brigada del INSNSB.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal de la Brigada responsable de las acciones de prevención y ejecución de la contingencia.
- Lista actualizada de funcionarios.}
- Copias de seguridad.

En la contingencia:



1. Desconectar el fluido eléctrico del centro de cómputo de ser necesario de todo el INSNSB.
2. Evacuar las instalaciones de acuerdo a las disposiciones de la Brigada.
3. No usar ascensor.
4. Verificar que todos los funcionarios que laboran en el área se encuentren bien. En caso de ser necesario, brindar los primeros auxilios al personal afectado si fuese necesario.
5. Alejarse de las ventanas para evitar heridas por vidrios.

Después de la contingencia:

1. Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, instalaciones eléctricas, documentos, etc. Hacer inventario general de documentación, personal, infraestructura y equipos.
2. Limpieza de las áreas afectadas por el sismo.
3. Elaborar un reporte del estado de operatividad de los equipos de informáticos para identificar los que requieren cambio o soporte



técnico.

4. En caso de tener equipos con estado de operatividad buena, alistarlos y colocarlos en funcionamiento.
5. Priorizar el funcionamiento de equipos primero servidores y luego equipos de cómputo de acuerdo con las necesidades del INSNSB.

POR INUNDACIÓN

Usuario: Todas las áreas del INSNSB.

Descripción: Suspensión parcial del servicio por Inundación. Este riesgo se considera MODERADO por la suspensión parcial del servicio.

Protección:

- Sistema de monitoreo de Data Center (sensores de detección de aniegos)
- Sistema de Video vigilancia
- Copias de Seguridad Actualizadas

En la contingencia:

1. Informar a la Dirección de Tecnologías de la Información problema presentado.
2. Abrir Ticket de incidencia con GEPEHO.
3. Comunicar a Servicios Generales.
4. Desconectar el fluido eléctrico de las zonas afectadas.
5. Coordinar el traslado de equipos hacia otras áreas dentro de la institución no afectadas por la inundación.

Después de la contingencia:

1. Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, instalaciones eléctricas, documentos, etc. Hacer inventario general de documentación, personal, infraestructura y equipos.
2. Limpieza de las áreas afectadas por el sismo.
3. Elaborar un reporte del estado de operatividad de los equipos de informáticos para Identificar los que requieren cambio o soporte técnico.
4. En caso de tener equipos con estado de operatividad buena, alistarlos y colocarlos en funcionamiento.





POR INCENDIO

Usuario: Todas las áreas del INSNSB

Descripción: El riesgo de la suspensión total del servicio por incendio. Este riesgo se considera MODERADO por la magnitud de pérdidas que ocasiona.

Protección:

- Realizar inspecciones de seguridad informática.
- Mantener las conexiones seguras.
- Capacitaciones permanentes en el manejo de extintores.
- Acatar las indicaciones de la Unidad de Gestión de Riesgos.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal de la Brigada responsable de las acciones de prevención y ejecución de la contingencia.
- Mantener actualizados los extintores.
- Sistema contra incendios con detectores de humo y fuego que accionan un sistema de alarmas y de descarga automática de gases que apagan las llamas originadas en el Data center.
- Copias de seguridad actualizadas.

En la contingencia:

1. Informar a la Dirección de Tecnologías de la Información problema presentado
2. Desconectar el fluido eléctrico del Data Center y de ser necesario de todo el INSNSB.
3. Tratar de apagar el incendio con extintores.
4. Comunicar al personal de Servicios Generales y GEPEHO
5. Evacuar las oficinas de acuerdo a las disposiciones de la Brigada.

Después de la contingencia:

1. Evaluar los daños ocasionados al personal, a los bienes e instalaciones. En caso de daños al personal prestar asistencia médica inmediata.
2. Realizar un inventario general de equipos.
3. Elaborar un reporte del estado de operatividad de los equipos de cómputo tanto de usuarios para identificar los que requieren cambio o soporte técnico.
4. En caso de tener equipos con estado de operatividad buena,





alistarlos y colocarlos en funcionamiento, priorizar el funcionamiento de equipos primero servidores y luego equipos de cómputo que apoyan procesos de atención al ciudadano.

5.5.5. R7- Retrasos en el Proceso de Adquisición de Bienes o Servicios de la entidad relacionados con los Sistemas de Información y Comunicaciones

Usuario: Todas las áreas del INSNSB.

Descripción: Este riesgo se considera MODERADO, por la magnitud de pérdidas que ocasiona.

Protección:

- Monitoreo de Cumplimiento del Plan Anual de Adquisiciones
- Contar con copias de seguridad actualizadas

En la contingencia:

1. Informar a la Dirección de Tecnologías de la Información problema presentado.
2. En caso de tratarse de una Licencia o Actualización de software se emplearán versiones libres o de demo con la funcionalidad mínima para soportar los procesos críticos mientras se supere el problema o se realizará la restauración a la última versión estable.
3. En caso de tratarse de equipos informáticos se gestionará el alquiler de equipos, servicios en la nube o su repotenciación para soportar los procesos críticos mientras se supere el problema.
4. En caso de tratarse de servicios, se gestionarán adendas o complementos para cubrir la prestación de servicios mientras se realizan los trámites regulares.



Después de la contingencia:

1. Monitorear el cumplimiento de los procesos de Adquisición de Bienes y Servicios

5.5.6. R8 - Contratación sin asistencia técnica, de Soluciones de Software no compatibles frente a los Requerimientos y Recursos Disponibles.

Usuario: Todas las áreas del Instituto Nacional de Salud del Niño San Borja.

Descripción: El riesgo es MODERADO debido al impacto que tiene sobre la infraestructura de software sobre los cuales funcionan los aplicativos de la



Institución que soportan los procesos misionales de la entidad.

Protección: Personal calificado.

En la contingencia:

1. Levantar los nuevos requerimientos que no están implementados en el sistema afectado.
2. Realizar el levantamiento de información que correspondan a nuevos formularios o modificación de formularios del sistema de información afectado, indicando medio de entrega, plazo.
3. Solicitar a los usuarios mantener los registros que no pudieron ser ingresados para su posterior inserción al sistema.

Después de la contingencia:

1. Contactar al contratista que desarrolló o comercializó el sistema para concretar los ajustes necesarios a la contratación para subsanar las falencias presentadas.
2. Reportar al contratista respectivo los cambios o nuevos requerimientos del sistema afectado para su implementación.
Solicitar a los usuarios el ingreso de la información no registrada en el sistema.

5.5.7. R9 - Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción.

Usuario: Todas las áreas del Instituto Nacional de Salud del Niño San Borja.

Descripción: El riesgo de pérdida de información es un riesgo que se considera ALTO, por la magnitud de pérdidas que ocasiona.

Protección:

- Equipo Cortafuegos.
- Sistema antivirus en todos los equipos de cómputo y servidores.
- Sistema de almacenamiento masivo SAN

En la contingencia:

1. Identificar el usuario que reporta pérdida de información y la información requerida.
2. Verificar el estado de los cortafuegos y analizar el informe correspondiente.





3. Ejecutar el antivirus o sistema de detección de intrusión en el equipo del usuario.
4. Restaurar la copia de seguridad más reciente en el equipo afectado.

Después de la contingencia:

1. Evaluar el reporte de incidencias tanto del Cortafuegos como de la solución de antivirus.
2. Identificación del mecanismo utilizado que ocasionó la pérdida de la información.
3. Aplicación de reglas de seguridad que boqueen futuros accesos no autorizados a los equipos de la red.

5.5.8. R10 - Falla técnica en equipos servidores, de escritorio o de comunicaciones.

Usuario: Todas las unidades orgánicas de la Entidad, usuarios.

Descripción: El riesgo de falla técnica en equipos servidores es MODERADO si la falla se presenta en un equipo servidor que aloje servicios de correo, página web, carpetas compartidas debido al impacto que tiene sobre la información. Puede ocasionar pérdida de información y/o suspensión del servicio.

Protección equipos servidores

- Mantenimiento preventivo y correctivo del hardware y software de los equipos.
- Servicio de mantenimiento preventivo y correctivo de equipos y servidores vigentes (GEPEHO).
- Sistema de aire acondicionado en Data Center.
- Medios de instalación de los sistemas operativos, Controlador de dominio, DNS Y DHCP
- Copia de seguridad más reciente del sistema o servicio
- Copia de respaldo de las bases de datos y aplicaciones.



Protección equipos de cómputo

- Mantenimiento preventivo y correctivo de los equipos.
- Servicio de mantenimiento preventivo y correctivo de equipos y servidores vigentes (GEPEHO).
- Sistema de aire acondicionado en Data Center.



PERU

Ministerio
de Salud

Instituto Nacional de Salud
del Niño San Borja



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

En la contingencia:

Para servicios de red:

1. Desconectar de la red equipo servidor afectado.
2. Revisar el equipo afectado para identificar la parte que presenta la falla.
3. Cambiar la parte dañada o solicitarla al proveedor.
4. Instalar la nueva parte e instalar el software si es necesario.
5. Hacer pruebas al hardware.
6. Diagnosticar el estado del sistema operativo del equipo servidor.
7. De ser necesario reinstalar el software y las aplicaciones.
8. Hacer pruebas.
9. Conectar el servidor y subir los servicios.

Para el servicio de Correo:

1. Revisar el Sistema Operativo del Servidor afectado
2. Determinar que instancia de correo electrónico se ha visto afectada
3. Realizar el cambio hacia el servicio de contingencia de correo electrónico
4. Diagnosticar los servicios afectados y el estado de los mismos
5. Reiniciar los servicios de ser esto posible
6. Diagnosticar el estado del sistema operativo del servidor.
7. De ser necesario reinstalar el software y las aplicaciones.
8. Hacer pruebas.
9. Conectar el servidor y subir los servicios.



Para el portal web e intranet:

1. Desconectar el equipo de la red.
2. Restaurar en el equipo de soporte la copia de seguridad más reciente de bases de datos y sitios web.
3. Configurar los archivos correspondientes a la publicación del sitio web.
4. Revisar permisos de carpetas.
5. Cambiar la IP de equipo de soporte y colocar como IP la dirección pública.
6. Conectar a la red el equipo de soporte y colocarlo en producción.
7. Revisar el equipo afectado para identificar la parte que presenta la falla.
8. Cambiar la parte dañada o solicitarla al proveedor e instalarla.
9. Hacer pruebas al hardware.

08



10. Restaurar en el equipo afectado la copia de seguridad más reciente de bases de datos y sitios web.
11. Revisar permisos de carpetas.
12. Desconectar de la red el equipo de soporte.
13. Cambiar la IP de equipo reparado y colocar como IP pública.
14. Conectar a la red el equipo reparado.

Para servidor de archivos:

1. Desconectar de la red el equipo afectado.
2. Restaurar la copia de seguridad más reciente de las carpetas compartidas al servidor destinado como soporte.
3. Crear los permisos a cada carpeta compartida.
4. Verificar la existencia del servidor nuevo en el dominio.
5. Re direccionar de manera transparente para los usuarios la nueva ruta del servidor de archivos.
6. Revisar el equipo afectado para identificar la parte que presenta la falla.
7. Cambiar la parte dañada o solicitarla al proveedor e instalarla.
8. Hacer pruebas al hardware.
9. Instalar el software necesario del servicio afectado.
10. Restaurar la copia de seguridad más reciente de las carpetas compartidas y/o Intranet al servidor de archivos inicial.
11. Crear los permisos a cada carpeta compartida.
12. Re direccionar de manera transparente para los usuarios la ruta del servidor de archivos.
13. Conectar a la red el equipo inicial reparado.



Para servidores de aplicaciones críticas:

1. Desconectar de la red el equipo afectado.
2. Alistar equipo de respaldo para la aplicación crítica afectada.
3. Restaurar la copia de seguridad más reciente del aplicativo crítico correspondiente.
4. Crear los permisos a cada carpeta compartida.
5. Verificar la existencia del servidor nuevo en el dominio y colocarlo en producción.
6. Re direccionar de manera transparente para los usuarios la nueva ruta del servidor del aplicativo.
7. Revisar el equipo afectado para identificar la parte que presenta la falla.
8. Cambiar la parte dañada o solicitarla al proveedor e instalarla.
9. Hacer pruebas al hardware.
10. Instalar el software necesario del servicio afectado.



11. Restaurar la copia de seguridad más reciente del aplicativo afectado en el servidor inicial.
12. Verificar los permisos sobre el aplicativo.
13. Re direccionar de manera transparente para los usuarios la ruta del servidor del aplicativo.
14. Conectar a la red el equipo inicial reparado.

5.5.9. R12 - Ausencia de personal de la Unidad de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información.

Usuario: Todas las unidades orgánicas de la Entidad, usuarios

Descripción: El riesgo de ausencia de personal que brinda soporte y mantenimiento en aplicaciones críticas es ALTO, dado que puede generar suspensión parcial o total del servicio.

Protección:

- Contrato con personal especializado en la labor técnica.
- Manuales técnicos de aplicativos críticos
- Copia de respaldo de las bases de datos y aplicaciones.

En la contingencia

1. Evaluar el problema reportado por el personal afectado.
2. Identificar qué sistema o equipamiento se debe de atender.
3. Revisar los manuales técnicos correspondientes
4. Atender el requerimiento
5. Cerrar el caso de atención

Después de la contingencia:

1. Reportar a la jefatura correspondiente las acciones realizadas.

5.5.10. R13 - Mal uso de hardware y/o software por parte de los colaboradores del INSNSB.

Usuario: Todas las unidades orgánicas de la Entidad, usuarios

Descripción: El riesgo por mal uso de hardware y/o software es MODERADO, dado que puede afectar la operatividad de algún proceso de trabajo administrativo o asistencial.





Protección:

- Equipos de contingencia.
- Manuales de usuario para sistemas críticos
- Capacitaciones a usuarios finales sobre el uso del hardware y software
- Copia de respaldo de las bases de datos y aplicaciones.

En la contingencia

MAL USO DE HARDWARE

1. Desconectar de la red equipo servidor afectado.
2. Revisar el equipo afectado para identificar la parte que presenta la falla.
3. Cambiar la parte dañada o solicitarla al proveedor.
4. Instalar la nueva parte e instalar el software si es necesario.
5. Hacer pruebas al hardware.

MAL USO DE SOFTWARE

1. Desconectar de la red el equipo afectado.
2. Alistar equipo de respaldo para la aplicación crítica afectada.
3. Restaurar la copia de seguridad más reciente del aplicativo crítico correspondiente.
4. Crear los permisos de acceso.
5. Verificar la existencia del servidor nuevo en el dominio y colocarlo en producción.
6. Re direccionar de manera transparente para los usuarios la ruta del servidor del aplicativo.



5.5.11.R14 - Calentamiento del centro de cómputo

Usuario: Todas las áreas y unidades orgánicas de la institución.

Descripción: El riesgo del calentamiento del centro de cómputo se considera ALTO ya que al quedar inoperantes los sistemas de información, equipos servidores y equipos de comunicaciones se paralizan los servicios internos y externos.

Protección:

- Aire acondicionado en el Data Center.
- Equipos UPS
- Grupo electrógeno para servicios críticos
- Monitoreo del estado del aire acondicionado y de la



PERU

Ministerio
de Salud

Instituto Nacional de Salud
del Niño San Berta



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

temperatura de los equipos del centro de cómputo.

En la contingencia:

1. Apagar los equipos del centro de cómputo.
2. Revisar el funcionamiento del aire acondicionado.
3. Contactar al proveedor (GEPEHO) para informar el hecho.
4. Restaurar el correcto funcionamiento del aire acondicionado.
5. Iniciar los equipos del centro de cómputo.

5.6. Procedimiento del Plan de Contingencias de TI

No.	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL / OBSERVACIONES
1	Colaborador de la entidad	Reporta la falla al Equipo de Desarrollo del Plan de Contingencias de TI por teléfono o correo electrónico. Tiempo: Inmediato.		
2	Director de la Unidad de Tecnologías de la Información Coordinador del Plan de Contingencias	Dependiendo del tipo de falla que se presenta, asigna a un colaborador del Equipo de desarrollo del Plan, para que realice la verificación. Tiempo: Inmediato.		
3	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	Realiza visita en sitio al área donde se ha presentado la falla. Identifica, efectúa diagnóstico y emite concepto sobre la falla y determina su alcance. Tiempo de respuesta: Inmediato		





"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

4	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Inhabilita el uso del equipo o equipos sobre el cual funciona el sistema de Información crítico en cuestión e informa a los usuarios para que no desarrollen ninguna actividad en el sistema afectado.</p> <p>Registra la contingencia en el formato "Registro Plan de Contingencias de TI".</p> <p>Tiempo: Inmediato, Máximo 10 minutos</p>	Formato "Registro Plan de contingencias de TI"	
5	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Reporta la falla al Coordinador del Plan de Contingencias de TI. Esta debe contener como mínimo: <i>Tipo falla, sistema de información, área, descripción de la falla.</i></p> <p>Tiempo: Inmediato, Máximo 5 minutos</p>	Correo electrónico	
6	<p>Director de la Unidad de Tecnologías de la Información</p> <p>Coordinador del Plan de Contingencias</p>	<p>Autoriza la puesta en marcha del Plan de Contingencias de TI notificando a las áreas afectadas y al personal encargado de ejecutar las actividades del plan.</p> <p>Tiempo: Inmediato</p>	<p>Correo electrónico</p> <p>Formato "Registro Plan de Contingencias de TI".</p>	<p>PUNTO DE COTRNL:</p> <p>Se debe registrar la autorización en el anexo 1 formato Registro Plan de Contingencias de TI.</p>
7	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Implementa las actividades establecidas en el Plan de Contingencias de TI que correspondan para restablecer el sistema afectado.</p> <p>Tiempo: El mínimo dependiendo de la complejidad de la solución. No debe ser mayor a 5 horas.</p>		
8	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Reporta al Coordinador del Plan de Contingencias de TI la finalización de las actividades implementadas.</p> <p>Tiempo: Una vez finalizado entre 15 y 30 minutos.</p>	<p>Correo electrónico</p> <p>Formato Registro Plan de Contingencias de TI.</p>	<p>Observación:</p> <p>En caso de encontrar información adicional sobre el estado o las soluciones implantadas, incluirlas en el anexo 1 formato Registro Plan de Contingencias de TI.</p>





"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

10	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Realiza pruebas a la solución implementada y monitorea el funcionamiento del sistema.</p> <p>Registra las pruebas realizadas al sistema afectado.</p> <p>Tiempo: Observación permanente, mientras dure la contingencia</p>	Formato Registro Plan de Contingencias de TI.	<p>Punto de control:</p> <p>Se deben registrar las pruebas realizadas en el anexo 1 formato Registro Plan de Contingencias de TI.</p> <p>Observación:</p> <p>En caso de que los equipos hayan sido reemplazados, se debe iniciar las labores respectivas</p>
				(ubicar al proveedor, hacer efectivas las garantías, hacer soporte correctivo, contratar nuevas soluciones, etc.), que permitan reparar o restituir el elemento inicial afectado.
11	Profesional Especializado o colaborador del Equipo de Desarrollo del Plan.	<p>Informa al Coordinador del Plan de Contingencias de TI el restablecimiento del proceso en condiciones normales.</p> <p>Tiempo: Inmediato</p>	Correo electrónico	
12	<p>Director de la Unidad de Tecnologías de la Información</p> <p>Coordinador del plan</p>	<p>Autoriza la finalización y cierre del Plan de Contingencias e informa a las áreas afectadas la normalización del sistema o proceso.</p> <p>Registra la finalización del Plan de Contingencias de TI.</p> <p>Tiempo: Inmediato</p>	Correo electrónico	<p>Punto de Control:</p> <p>Registrar la firmeza quien autoriza el cierre en el anexo 1 formato Registro Plan de Contingencias de TI.</p>
13	Profesional Especializado o Universitario, del Grupo de Desarrollo del Plan.	<p>Actualiza Hoja de vida del equipo, servidor o del sistema de información sobre la incidencia presentada.</p> <p>Tiempo: Una vez solucionada la contingencia.</p>	Formato Hoja de vida del equipo o del Sistema de información.	





5.7. Plan de Pruebas

El plan de pruebas tiene como objetivo reducir la probabilidad de riesgos a un nivel aceptable asegurando la continuidad de los sistemas de información críticos de la Institución, del hardware y/o del software y la adecuada recuperación de la información. Las pruebas deben ser registradas en el formato Pruebas Plan de Contingencias de TI.

El Plan de Contingencias de TI del INSNSB debe de tener por lo menos una prueba al año. La prueba dependerá de lo que se quiera ensayar y consiste en llevar a cabo simulacros de:

1. Recuperación de la información de las copias de seguridad para verificar su correcto proceso de restauración.
2. Puesta en producción de los equipos de respaldo de los sistemas de información críticos de la Institución.
3. Pruebas de suministro de energía eléctrica con UPS y Grupo Electrónico.
4. Pruebas de alternancia de los equipos de aire acondicionado.
5. Pruebas de la conexión alterna del Servicio de Internet.

1. Prueba de restauración de información

Consiste en realizar una restauración de los resguardos periódicos más recientes que se tienen de los aplicativos críticos, en otro servidor utilizando los procedimientos existentes de restauración. Esta prueba brinda la garantía de que los resguardos son utilizables.

Las pruebas de restauración de información se registran en el formato Pruebas del Plan de Contingencias de TI.

2. Prueba puesta en producción de los equipos de respaldo

Consiste en levantar uno o más de los servicios de los servidores principales en los servidores de respaldo, restaurar los datos y ejecutar el sistema de información crítico, con el fin de verificar el funcionamiento de los aplicativos críticos en un servidor de respaldo.

Las pruebas de puesta en producción de los equipos de respaldo se registran en el formato de Pruebas del Plan de Contingencias de TI.

3. Prueba de Suministro de Energía Eléctrica con UPS y Grupo Electrónico

Los UPS son el sistema que garantiza la energía eléctrica a los equipos del Data Center y Cuartos de Comunicaciones cuando haya una suspensión del servicio eléctrico.





El Grupo Electrónico es el sistema que garantiza la energía eléctrica a los sistemas críticos de la institución cuando haya una suspensión del servicio eléctrico.

Esta prueba se realiza manteniendo los equipos de cómputo y servidores activos, se corta el fluido eléctrico que viene de la empresa suministradora de energía. Esta prueba permite probar la autonomía que tienen los UPS, la cual se espera sea de 60 minutos en el Data Center y 10 minutos en los cuartos de comunicaciones, dando tiempo para el encendido y operatividad del grupo electrónico y caso contrario el apagado controlado del equipamiento.

Las pruebas de Suministro de Energía Eléctrica se registran en el formato de Pruebas del Plan de Contingencias de TI.

4. Pruebas de alternancia de equipos de aire acondicionado

Se cuenta con dos equipos de aire acondicionado que abastecen el Data Center, los cuales mantienen la temperatura del ambiente en condiciones óptimas para el buen funcionamiento del equipamiento.

Esta prueba se realiza apagando uno de los dos equipos de aire acondicionado a la espera del encendido automático del equipo alterno.

Las pruebas de alternancia de equipos de aire acondicionado se registran en el formato de Pruebas del Plan de Contingencias de TI.



5. Pruebas de la conexión alterna del Servicio de Internet.

Se cuenta con dos enlaces contratado para este servicio en modalidad activo pasivo, mediante este esquema se busca minimizar el tiempo de interrupción posible del servicio.

Esta prueba se realiza deshabilitando uno de los enlaces a la espera de la activación automática del enlace pasivo.

Las pruebas de conexión alterna del servicio de internet se registran en el formato de Pruebas del Plan de Contingencias de TI.



5.8. Actualización del Plan

Este documento debe ser revisado y si es necesario actualizarlo cada vez que se ejecuta una parte del plan o todo el plan. Así mismo, es necesario actualizarlo al presentarse lo siguiente:

- Se realizaron las pruebas establecidas de conectividad, energía eléctrica, restauración de información, puesta en marcha de servidores alternos y se hicieron ajustes.
- Se adquirió nueva infraestructura tecnológica (hardware o software).
- Puesta en ejecución y finalización del Plan de Contingencias de TI.
- Surjan cambios o acciones correctivas al plan.
- Cambios en la identificación y análisis de los riesgos.

6. VARIABLES TÉCNICAS A TENER EN CUENTA EN LA IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIAS DE TI

El plan aplica a las actividades necesarias para mantener en operatividad los servicios informáticos considerados críticos.

Para su implementación es necesario tener en cuenta aspectos técnicos, humanos y logísticos que nos permitan estar preparados para afrontar la contingencia.

Los componentes de hardware, software o conectividad que aplican son:

TÉCNICOS

- Recursos Técnicos Contingencia Aplicaciones Críticas (SIGA, SIAF, SisGalenPlus)
 - Servidor(es) de Contingencia
 - Hardware
 - Memoria: 8 GB
 - Disco Duro : 1 Tb
 - Procesador Xeon mínimo 6 núcleos
 - Software
 - Sistema Operativo Windows Server 2012 / SQL Server 2012
 - Backups de Base de Datos
- Recursos Técnicos Contingencia Servidor de Base de Datos
 - Servidor de Contingencia
 - Hardware
 - Memoria: 16 GB





"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

- Disco Duro : 1 Tb
- 2 Procesadores Xeon mínimo 6 núcleos
- Software
 - Sistema Operativo Windows Server 2012 / SQL Server 2012
- Backups de Base de Datos

HUMANOS

- Un administrador de Base de Datos
- Un administrador de Plataforma (Servidores, Sistemas Operativos y Conectividad)

Se requiere contar con personal que tenga conocimientos claros de la administración de las bases de datos, sistemas operativos y conectividad. Lo anterior con el fin de dar soporte a las tareas de implementación de la puesta en marcha del sistema de información crítico que se encuentra en contingencia.

LOGÍSTICA

- Servicio de Data Center Alterno
- Servicio de Custodia Externa de Copias de Seguridad

7. RECOMENDACIONES

- Verificar periódicamente el directorio telefónico de contacto del personal responsable del plan y mantenerlo actualizado.
- Verificar los procedimientos de copia y restauración de las copias de seguridad.
- Realizar jornadas de capacitación sobre el plan, al personal de las diferentes áreas sobre las actividades a seguir en el proceso de contingencia.
- Contratar el servicio de Data Center alternativo.
- Contratar el servicio de Custodia Externa de Copias de Seguridad





PERÚ

Ministerio
de Salud

Instituto Nacional de Salud
INSA



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"

8. ANEXOS

Anexo 1. Formato de registro Plan de Contingencias de TI

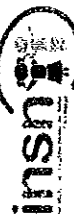
PLAN DE CONTINGENCIAS DE TI									
REGISTRO DE ACTIVACION DEL PLAN DE CONTINGENCIAS DE TI									
Nº	Fecha activación	Hora activación	Dependencia del Colaborador que Informa	Colaborador que Informa	Descripción de la contingencia	Firma de quien autoriza la activación	Hora Finalización	Firma de quien autoriza el cierre	Observaciones
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									





PERÚ

Ministerio
de Salud



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"



INSTRUCCIONES PARA LLENADO DE ANEXO 1	
Campo	Descripción
1. Fecha activación	Formato dd/mm/yyyy
2. Hora activación	Formato 24 horas, ejemplos 8:00 / 17:00.
3. Dependencia que informa la contingencia	Nombre del Area/Servicio donde fue detectada la contingencia
4. Colaborador que informa	Nombre y apellidos del colaborador que informa la contingencia
5. Descripción de la contingencia	Escribir detalles de la contingencia presentada incluyendo nombre del servicio afectado y una descripción breve del problema más relevante que se presenta
6. Firma del quien autoriza la activación	Firma del director, o colaborador que autoriza la activación del Plan de Contingencias de TI.
7. Hora de finalización de la contingencia	Formato 24 horas, ejemplos 8:00 / 17:00.
8. Firma de quien autoriza el cierre	Firma del director, o colaborador que autoriza el cierre del Plan de Contingencias de TI.
9. Observaciones	En caso de encontrar información adicional sobre el estado del plan o de las soluciones implementadas, incluirlas en este campo.



**“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año del Diálogo y la Reconciliación Nacional”**

Anexo 2. Formato de pruebas del Plan de Contingencias de TI



PRUEBAS DEL PLAN DE CONTINGENCIAS DE TI

Fecha:

Hora:

Lugar:

[illegible]

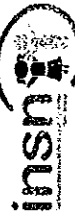
Dirigido por

Verificado por



PERÚ
Ministerio
de Salud

Instituto Nacional de Salud
del Perú



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Diálogo y la Reconciliación Nacional"



INSTRUCCIONES PARA LLENADO DE ANEXO 2	
Campo	Descripción
1. Fecha	Formato dd/mm/YYYY
2. Hora	Formato 24 horas, ejemplos 8:00 / 17:00.
3. Lugar	Nombre del Area/Servicio donde se realizaron las pruebas
4. Tipo de prueba	Escribir alguno de los siguientes tipos: Prueba de restauración de información Prueba puesta en producción de los equipos de respaldo Prueba de Suministro de Energía Eléctrica con UPS y Grupo Electrogeno Pruebas de alternancia de equipos de aire acondicionado Pruebas de la conexión alterna del Servicio de Internet
5. Actividades desarrolladas	Relación de actividades técnicas que se realizan dentro de las pruebas de acuerdo al tipo de prueba, por ejemplo: Si la prueba es RECUPERACION DE INFORMACION una actividad sería borrado de información de la carpeta compartida y otra es la restauración de la copia de respaldo más reciente
6. Personal que participó	Relación de colaboradores y/o entidades que participaron
7. Resultado esperado	Formato 24 horas, ejemplos 8:00 / 17:00
8. Resultado obtenido	Descripción de los resultados de la ejecución del plan. En el ejemplo hubiera podido ser Fallos en el proceso de restauración, o información de la copia de respaldo muy desactualizada
9. Duración de prueba	Tiempo en horas invertido en la realización de las pruebas
10. Observaciones	En caso de encontrar información adicional como recomendaciones o aclaraciones
11. Dirigido por	Firma del director, o colaborador que dirigió la ejecución del Plan de Pruebas
12. Verificado por	Firma del director, o colaborador que constató la ejecución del Plan de Pruebas