GOBIERNO REGIONAL
MOQUEGUA

Nº 395-2023-DIRESA-HRM/DE

Resolución Ejecutiva Directoral

Moquegua, 01 de diciembre de 2023.

VISTOS: El Informe N° 168-2023-DIRESA-HRM/01-0/EMED emitido el 30 de noviembre de 2023 por el Área de Espacios de Monitoreo Emergencia y Desastres, el Informe N° 503-2023-DIRESA-HRM-AL/01 emitido el 28 de noviembre de 2023 por el Área de Asesoria Legal, el Informe N° 1465-2023-HRM-03 emitido el 21 de noviembre de 2023 por la Jefatura de la Oficina de Planeamiento Estratégico, el Informe N° 244-2023-DIRESA-HRM/03-0/PLAN emitido el 21 de noviembre de 2023 por el Área de Planeamiento, el Informe N° 159-2023-GRM-DIRESA/DR-UFEI emitido el 14 de noviembre de 2023 por la Unidad Funcional de Estadística e Informática de la DIRESA, el Informe N° 553-2023-DIRESA-HRM-01 emitido el 16 de octubre de 2023 por la Dirección Ejecutiva del Hospital Regional de Moquegua, el Informe N° 508-2023-DIRESA-HRM/07 emitido el 06 de octubre de 2023 por la Unidad de Estadística e Informática, el Informe N° 0327-2023-DIRESA-HRM/07-0/INFMAT emitido el 05 de octubre de 2023 por el Área de Informática, el Informe N° 202-2023-DIRESA-HRM/03-0/PLAN emitido el 19 de septiembre de 2023 por el Área de Planeamiento, el Informe N° 137-2023-DIRESA-HRM/01-0/EMED emitido el 08 de septiembre de 2023 por el Área de Espacios de Monitoreo Emergencias y Desastres, el Informe N° 512-2023-DIRESA-HRM/05 emitido el 13 de julio de 2023 por la Unidad de Gestión de la Calidad, el Informe N° 250-2023-DIRESA-HRM/07 emitido el 23 de mayo de 2023 por la Unidad de Estadística e Informática, el Informe N° 202-2023-DIRESA-HRM/07-0/INFMAT emitido por el responsable del Área de Informática, y;

CONSIDERANDO:

Que, mediante Resolución Ejecutiva Regional N° 0101-2011-GR/MOQ, del 15 de febrero del 2011, se resuelve crear la Unidad Ejecutora 402 Hospital Regional de Moquegua, en el Pliego N° 455 Gobierno Regional del Departamento de Moquegua, para el logro de objetivos y la contribución de la mejora de la calidad y cobertura del servicio público de salud y que por la función relevante la administración de la misma requiere independencia para garantizar su operatividad, teniendo como representante legal a su director;

Que, el numeral XV del Título Preliminar de la Ley N° 26842, Ley General de Salud, establece que, el Estado promueve la Investigación Científica y Tecnológica en el campo de la salud, así como la formación, capacitación y entrenamiento de recursos humanos para el cuidado de la salud;

Que, mediante Resolución Ministerial N° 431-2015/MINSA de fecha 09 de julio de 2015, se aprobó el documento técnico "Política de Seguridad de la Información del Ministerio de Salud MINSA", con la finalidad de mantener la continuidad de las operaciones del Ministerio de Salud, en relación a los sistemas de información seguros, minimizando sus riesgos y maximizando los niveles de satisfacción de los usuarios; siendo su objetivo de establecer los principios para la implementación del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud;

Que, a través de Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 2700:2014, denominada "Tecnología de Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición", la mencionada Norma Técnica Peruana ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. Asimismo, se tiene que el objetivo de la mencionada norma incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización;

Que, con Resolución Ministerial N° 028-2015-PCM, se aprueba los "Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno", cuya finalidad es establecer los procedimientos específicos que permitan garantizar que ante un desastre de gran magnitud o cualquier evento que interrumpa prolongadamente las operaciones de las Entidades Públicas, se cuente con una planificación para la continuación de las actividades criticas de su competencia;

Que, mediante Resolución Ejecutiva Directoral N° 174-2016-DRSM-UEHRM/DE, se aprueba el esquema para elaborar planes de las Unidades Orgánicas del Hospital Regional de Moquegua;

MOQUEGUA

Nº 395-2023-DIRESA-HRM/DE

Resolución Ejecutiva Directoral

Moquegua, 01 de diciembre de 2023.

Que, mediante Informe N° 250-2023-DIRESA-HRM/07 de fecha 23 de mayo de 2023, la Unidad de Estadística e Informática, remite ante la Dirección Ejecutiva del Hospital Regional de Moquegua, el proyecto del "Plan de Contingencia Informático – 2023", elaborado por el Área Funcional de Informática, para la revisión, evaluación y aprobación mediante acto resolutivo;

Que, con Informe N° 512-2023-DIRESA-HRM/05 de fecha 13 de julio de 2023, la Unidad de Gestión de la Calidad, recomienda que el plan sea derivado al Área de Espacios de Monitoreo de Emergencias y Desastres (EMED), para su atención correspondiente. Siendo que, A través de Informe N° 137-2023-DIRESA-HRM/01-0/EMED de fecha 08 de septiembre de 2023, el Área de Espacios de Monitoreo de Emergencias y Desastres (EMED), sugiere se derive a la Oficina de Planeamiento Estratégico, para su revisión.

Que, mediante Informe N° 202-2023-DIRESA-HRM/03-0/PLAN de fecha 19 de septiembre de 2023, el Área de Planeamiento, advierte observaciones al plan de contingencia informático, por lo que lo devuelve a fin de que se subsane, siendo la observación que, el mencionado plan no cumpliría con el Esquema para elaborar planes de contingencia, aprobado con Resolución Ministerial N° 643-2019/MINSA, que aprueba la "Directiva administrativa N° 271-MINSA/2019/DGERD "Directiva administrativa para la formulación de planes de contingencia de las entidades e instituciones del sector salud";

Que, con Informe N° 508-2023-DIRESA-HRM/07 de fecha 10 de octubre de 2023, la Unidad de Estadística e Informática, remite el Informe N° 327-2023-DIRESA-HRM/07-0/INFMAT, mediante el cual el Área de Informática, requiere se eleve en consulta o se reciba asistencia técnica competente en elaboración de planes de contingencia relacionado a temas de tecnologías de la información y comunicaciones, con la finalidad de que se oriente correctamente la formulación del plan de contingencia informático del Hospital Regional de Moquegua;

Que, en merito a lo requerido por las áreas técnicas, la Dirección Ejecutiva a través de Informe N° 553-2023-DIRESA-HRM-01 de fecha de recepción 30 de octubre de 2023, remite en consulta ante la DIRESA, el Plan de Contingencia Informática 2023 del Hospital Regional de Moquegua;

Que, con Informe N° 159-2023-GRM-DIRESA/DR-UFEI de fecha 14 de noviembre de 2023, la Unidad Funcional de Estadística e Informática de la DIRESA, remite el Informe N° 011-2023-GRM-DIRESA/DR-UFEI-REGV mediante el cual emite opinión respecto al plan de contingencia, precisando que no hay observación de fondo ni de forma, sin embargo, se debe tener en cuenta las normas especializadas en temas informáticos, INEI, la NTP ISO/IEC 27001:2014, RJ 347-2001-INEI, RJ 386-2002-INEI, entre otras;

Que, a través de Informe N° 1465-2023-DIRESA-HRM-03 de fecha 22 de noviembre de 2023, la Oficina de Planeamiento Estratégico, deriva el Informe N° 244-2023-DIRESA-HRM/03-0/PLAN del Área de Planeamiento, del cual se extrae la siguiente conclusión: De acuerdo a las opiniones vertidas por la Unidad Funcional de Estadística e Informática de la Dirección Regional de Salud Moquegua – DIRESA, **emite opinión favorable**; asimismo, recomienda que, previa a su aprobación, se realice la revisión efectiva del Área de Espacios de Monitoreo Emergencias y Desastres del Hospital Regional de Moquegua, así como de la Unidad de Gestión de la Calidad; motivo por el cual, mediante Informe N° 503-2023-DIRESA-HRM-AL/01 de fecha 28 de noviembre de 2023, el Área de Asesoria Legal, solicita previa a la elaboración de la resolución de aprobación, se derive el expediente a las mencionadas áreas;

Que, el Área de Espacios de Monitoreo Emergencias y Desastres, con Informe N° 168-2023-DIRESA-HRM/01-0/EMED de fecha 30 de noviembre de 2023, indica que, el mencionado plan no corresponde a los planes de contingencia que realiza el EMED, razón por la cual lo devuelve para su trámite correspondiente;

Contando con el visto bueno de la Oficina de Planeamiento Estratégico, la Unidad de Gestión de la Calidad, la Unidad de Estadística e Informática y con el proveído de Dirección Ejecutiva, que dispone la emisión del acto resolutivo.

GOBIERNO REGIONAL
MOQUEGUA

Nº 395-2023-DIRESA-HRM/DE

Resolución Ejecutiva Directoral

Moquegua, 01 de diciembre de 2023.

En atención a la Ley N° 27783 Ley de Bases de la Descentralización y en uso de las atribuciones conferidas en el inciso c) del Artículo 8° del Reglamento de Organización y Funciones (R.O.F.) del Hospital Regional de Moquegua aprobado con Ordenanza Regional N° 007-2017-CR/GRM;

SE RESUELVE:

Artículo 1°.- APROBAR el **"PLAN DE CONTINGENCIA INFORMATICO - 2023"** del Hospital Regional De Moquegua, el cual consta de cuarenta y ocho (48) folios y forma parte integrante de la presente resolución.

Artículo 2°.- ENCARGAR a la Unidad de Estadística e Informática, la difusión, monitoreo y evaluación del plan aprobado con la presente resolución.

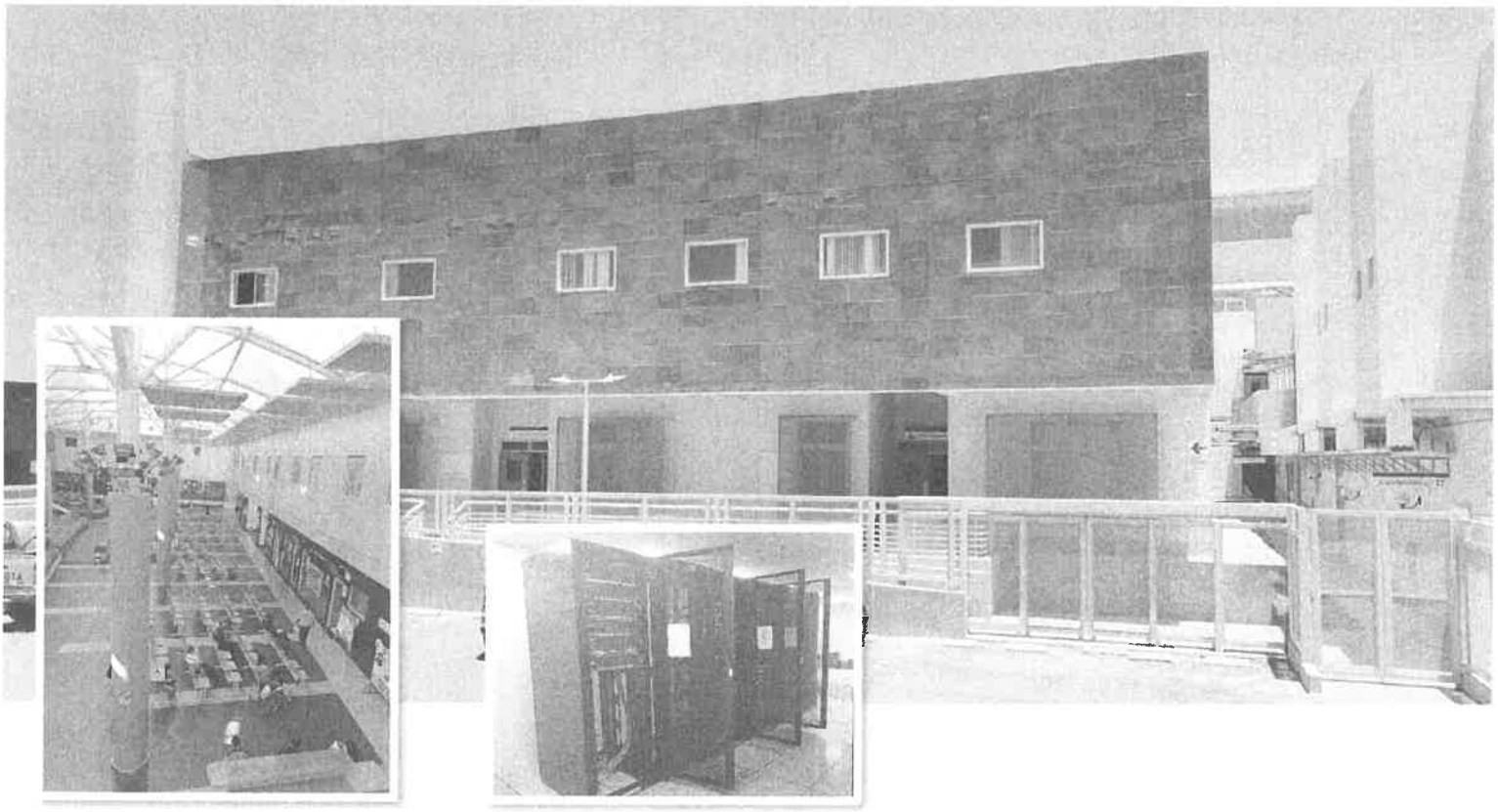
Artículo 3°.- REMÍTASE copia a la Unidad de Estadística e Informática, para su respectiva publicación en la página web Hospital Regional de Moquegua (www.hospitalmoquegua.gob.pe).

REGÍSTRESE, COMUNÍQUESE Y PUBLÍQUESE.

HOSPITAL REGIONAL DE MOQUEGUA
M.E. IDANIA EDITH MAMANI PILCO
C.M.P. 53129 RNE. 042740
DIRECTORA EJECUTIVA

IEMP/DIRECCIÓN
JLRV/AL
(01) O. ADMINISTRACION
(01) O. PLANEAMIENTO
(01) U.E.I
(01) U.G.C
(01) ESTADÍSTICA
(01) ARCHIVO

PLAN DE CONTINGENCIA INFORMÁTICO



UNIDAD DE ESTADÍSTICA E INFORMÁTICA

AREA DE INFORMÁTICA

2023

CONTENIDO

ÁREA DE INFORMÁTICA HRM

PLAN DE CONTINGENCIA INFORMÁTICO - 2023

I. INTRODUCCIÓN

El Hospital Regional de Moquegua cuenta con procesos administrativos y asistenciales que se apoyan en las Tecnologías de la Información y Comunicaciones (TIC), para ello posee una de las más avanzadas infraestructuras tecnológicas del sur del país, con alrededor de veinte subsistemas que conforman el sistema de comunicaciones hospitalario.

El Área de Informática de la Unidad de Estadística e Informática es la encargada de velar por la disponibilidad, continuidad, respaldo y seguridad del software, hardware e información para brindar los servicios informáticos a los usuarios internos y externos, y garantizar la continuidad de los mismos.

El Plan de Contingencia Informático constituye un instrumento de gestión para el correcto y óptimo manejo de las Tecnologías de la Información y Comunicaciones (TIC) frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma y los usuarios.

El presente plan está destinado a establecer medidas de protección de los sistemas, así como un protocolo de responsabilidades específicas de actuación para responder a la ocurrencia de eventos que materialicen el riesgo y así permitir la recuperación, en el más corto tiempo, de las operaciones y capacidades para procesar la información; más aún después de haber experimentado las consecuencias de la emergencia sanitaria por la pandemia a causa del COVID-19.

El Plan de Contingencia Informático es administrado por el Área de Informática del Hospital Regional de Moquegua, es fuente de consulta y aplicación para atender situaciones de contingencia, permitiendo restaurar los sistemas y/o servicios informáticos, ya sean asistenciales o administrativos, por algún inconveniente que pudiera presentarse con los mismos.

II. BASE LEGAL

- Ley Nº 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

- Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 26842, Ley General de Salud.
- Ley N° 29414, Ley que establece los derechos de las personas usuarias de los servicios de salud.
- Decreto Supremo N° 018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Resolución de Contraloría N° 146-2019-CG, que Aprueba la Directiva N° 006 -2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del Estado".
- Resolución Ministerial N° 431-2015/MINSA, que aprueba el Documento Técnico "Políticas de Seguridad de la Información del Ministerio de Salud"
- Resolución Ministerial N° 004-2016-PCM - Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 028-2015-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.
- Resolución Ejecutiva Directoral N° 174-2016-DRSM-UEHRM/DE – Aprueba el Esquema para elaborar planes de las unidades orgánicas del Hospital Regional de Moquegua.
- Resolución Ejecutiva Directoral N° 027-2023-DIRESA-HRM/DE – Aprueba el Plan Operativo Institucional (POI) Anual 2023 del Hospital Regional de Moquegua.

ÁREA DE INFORMÁTICA HRM

III. FINALIDAD

Contar con un plan de contingencia objetivo e integral, en el que se definen los procedimientos necesarios para afrontar cualquier ocurrencia que se produzca en los sistemas de información y los sub sistemas del sistema de comunicaciones del Hospital Regional de Moquegua, de tal forma que se garantice la continuidad, seguridad y confiabilidad de los mismos.

IV. OBJETIVOS

- **GENERAL**

  Garantizar la continuidad de los servicios informáticos que soportan los procesos del Hospital Regional de Moquegua, ante eventos que pudieran afectar el normal funcionamiento de los sistemas de información y comunicaciones, que a su vez involucren a procesos críticos del hospital y, se logre en el menor tiempo posible la recuperación del control de las operaciones y las capacidades para procesar la información en el hospital.

- **ESPECÍFICOS**

  1. Identificar y analizar los posibles riesgos que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones del hospital.
  2. Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
  3. Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.
  4. Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

V. RESPONSABLES DE LA FORMULACIÓN DEL PLAN

N°	Apellidos y Nombres	Cargo	Correo Electrónico	Teléfono
01	Elías Quispe Katherine De los Milagros	Responsable del Área de Informática	kelias@hospitalmoquegua.gob.pe	997003355
02	Cuevas Machaca Ronald Zenón	Ingeniero de Sistemas	rzcuevasm@hospitalmoquegua.gob.pe	--
03	Limache Melendez Ruth Mariela	Ingeniero de Sistemas	rlimache@hospitalmoquegua.gob.pe	--
04	Stelman Uribe Suge Milagros	Ingeniero de Sistemas	sstelman@hospitalmoquegua.gob.pe	--

VI. SIGLAS Y ACRÓNIMOS

EMED : Espacios de Monitoreo de Emergencias y Desastres
HRM : Hospital Regional de Moquegua
MINSA : Ministerio de Salud
TIC : Tecnologías de la Información y las Comunicaciones
UEI : Unidad de Estadística e Informática
VPN : Red Privada Virtual

VII. DEFINICIONES

- **Activo:** Son todos aquellos recursos o componentes de la entidad, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación.

- **Activo Informático:** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la entidad.

- **Amenaza:** Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la entidad.

- **Aplicativos:** Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.

- **Base de Datos:** Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios de selección.

- **Centro de Datos:** Es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

- **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.

- **Contingencia:** Interrupción, no planificada, de la disponibilidad de recursos informáticos. Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una entidad.

- **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- **Cortafuego (Firewall):** Es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

- **Cuarto de comunicaciones:** Es el área exclusiva dentro de un edificio para albergar los equipos de la red local de interconexión entre cada uno de los subsistemas del cableado estructurado. Su función principal de este elemento es la terminación del cableado horizontal y vertical y la interconexión entre ambos.

- **Datos:** Todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados y se presentan en forma de imágenes, sonidos o colección de bits.

- **Datos Personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

- **Impacto:** Es el grado de daño que el problema causará a la entidad. El impacto del incidente es el alcance de las consecuencias negativas en la entidad, sus usuarios, sus partes interesadas y su reputación.

- **Incidente:** Situación en la que se interrumpe la provisión de un servicio de TIC a los usuarios, impactando en la ejecución de las actividades y/o procesos de las áreas involucradas. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en el hospital.

- **Método de análisis de riesgos:** Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

- **Plan de Contingencia Informático:** Es un documento que establece un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la entidad.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas: Antes, como un plan de prevención para mitigar los incidentes. Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente. Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

- **Plan de Prevención:** Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

- **Plan de Ejecución:** Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

- **Plan de Recuperación:** Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

- **Plan de Pruebas:** Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

- **Probabilidad:** Posibilidad que un evento determinado ocurra en un período de tiempo dado.

- **Proceso crítico:** Proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.

- **Riesgo:** Se define como la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de la entidad.

- **Servicios informáticos:** Conjunto de actividades que buscan responder a las necesidades de los usuarios en una entidad, a consecuencia de un cambio en la condición o estado de un activo informático.

- **Sistemas de Información:** Conjunto de elementos relacionados entre sí con un objetivo en común, en el cual se almacenan datos y se genera información relacionada a un tema en particular, para ponerlos a disposición de sus usuarios. Pueden ser registros simples como archivos de ofimática, o pueden ser complejos como una aplicación de software con base de datos.

- **Tecnologías de la Información y Comunicaciones:** Son el conjunto de herramientas y recursos que nos permiten crear, gestionar, transmitir y utilizar información, como: voz, datos, texto, video e imágenes, a través de medios electrónicos.

- **Vulnerabilidad:** Debilidad de un activo, grupo de activos o controles, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.

VIII. CARACTERIZACIÓN DEL PLAN

8.1 IDENTIFICACIÓN DE NECESIDADES

El Hospital Regional de Moquegua, como establecimiento que brinda servicios para garantizar el derecho a la salud de la población, necesita contar de forma ininterrumpida con los servicios informáticos que soportan sus actividades; en esa orientación, se ha identificado las siguientes necesidades que el presente plan debe cubrir para el logro de sus objetivos:

- Se cuenta con 19 subsistemas que conforman el sistema de comunicaciones, que necesitan funcionar de forma ininterrumpida, para dar soporte a las actividades administrativas y asistenciales del hospital.
- La infraestructura tecnológica y el parque informático que posee el hospital, para la gestión de la información, deben funcionar de forma óptima sin que afecten la continuidad de los servicios hospitalarios.
- La información que se genera y almacena, de acuerdo a su necesidad, deber ser accesible a los usuarios internos y externos, garantizando su prontitud, integridad y confiabilidad.
- Se necesita contar con personal técnico y especializado para afrontar contingencias que afecten a los servicios informáticos del hospital.

8.2 PRIORIZACIÓN DE NECESIDADES

La continuidad de los servicios informáticos, determinan en parte, la continuidad de los servicios administrativos y asistenciales del hospital; en consecuencia, la totalidad de las necesidades identificadas, se priorizan y abordarán con la aprobación y ejecución del presente plan.

8.3 DEFINICION DE ACTIVIDADES

El desarrollo del presente plan seguirá una metodología basada en siete (07) fases:

- FASE 1: Planificación
- FASE 2: Determinación de vulnerabilidades y escenarios de contingencia
- FASE 3: Estrategias del Plan de Contingencia Informático
- FASE 4: Elaboración del Plan de Contingencia Informático
- FASE 5: Definición y Ejecución del Plan de Pruebas
- FASE 6: Implementación del Plan de Contingencia Informático
- FASE 7: Monitoreo

Fases que recogen algunos criterios señalados en la Directiva de Implementación del Sistema de Control Interno en las Entidades del Estado (2019) de la Contraloría General de la República. Así mismo, se ha hecho uso de la metodología heurística, de fácil implementación, con cuadros y matrices que combinan lo cuantitativo con lo cualitativo, donde lo fundamental es la asignación de las ponderaciones y/o valores a las variables e indicadores y los criterios técnicos de los profesionales en ingeniería que conforman el Área de Informática.

A continuación, se detalla cada fase:

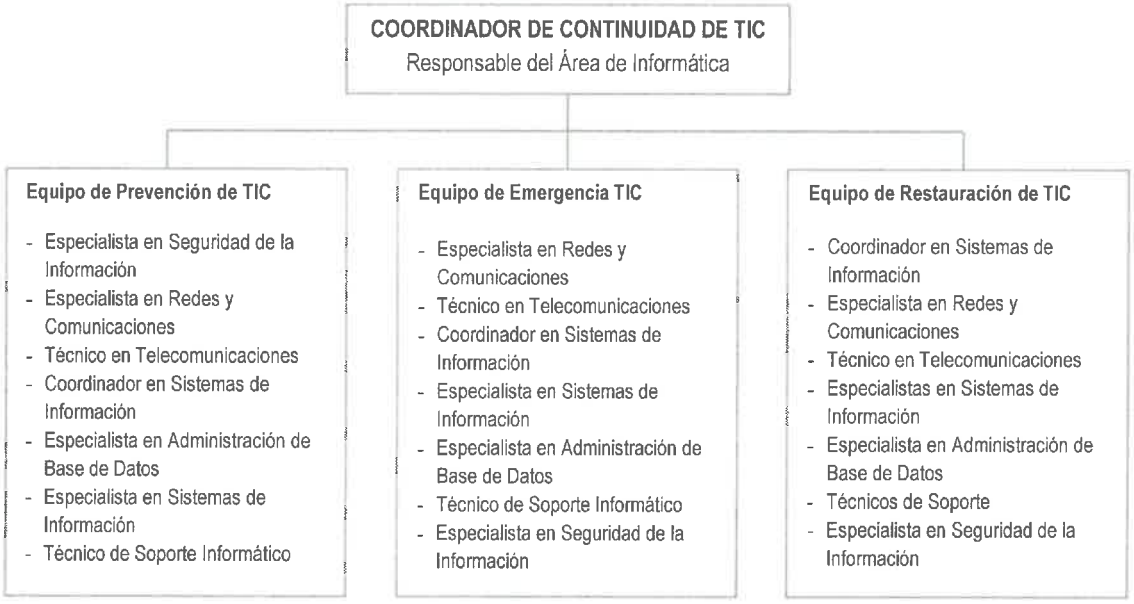
8.3.1 FASE 1: PLANIFICACIÓN

8.3.1.1 Organización

El Área de Informática depende de la Unidad de Estadística e Informática (UEI), y tiene dentro de sus actividades administrar la integridad, confiabilidad, y seguridad en el acceso a la información del hospital, así como establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a las base de datos; además de diseñar, construir, implantar, mantener los sistemas de información e infraestructura tecnológica necesaria para el cumplimiento de los objetivos del hospital, así como asegurar su disponibilidad y brindar soporte a los mismos.

Para el funcionamiento del Plan de Contingencia Informático, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal del Área de Informática.

Figura N° 01: Organización Operativa del Plan de Contingencia Informático



El/la responsable del Área de Informática, designa un miembro titular y opcionalmente un alterno, por cada integrante de los TRES (03) equipos detallados en la Figura N° 01. Para tal efecto, se debe contar con la relación del personal del Área de Informática que formarán estos equipos y que serán convocados en el momento de la contingencia.

Para garantizar las comunicaciones con los equipos a conformar, el/la responsable del Área de Informática debe tener operativo y funcionando, las 24 horas del día, el teléfono móvil asignado por el hospital, sobre todo para las comunicaciones fuera de la jornada laboral establecida; en ese sentido, obligatoriamente se adquirirá dispositivos de radio comunicación, como alternativa que garantice al 100% las comunicaciones con la totalidad del personal de los equipos. Así mismo, la relación del personal del Área de Informática que forma parte del Plan de Contingencia Informático se deberá actualizar de manera permanente, incluyendo números telefónicos, correos electrónicos, direcciones de sus domicilios y socializada al siguiente personal:

- Personal de la Unidad de Estadística e Informática.
- Personal del Grupo de Trabajo de Gestión del Riesgo de Desastres.

- Personal de la Alta Dirección.
- Central de Videovigilancia / Casetas de vigilancia.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en trabajo remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes.

8.3.1.2 Roles, funciones y responsabilidades dentro del Plan

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático.

Luego de aprobado el presente plan, el/la responsable del Área de Informática, asignará los roles entre los integrantes del equipo del Área de Informática, los cuales, dependiendo de la necesidad, podrán asumir más de un rol en uno o más equipos detallados en la Figura N° 01.

ÁREA DE INFORMÁTICA HRM

a. Coordinador de Continuidad de TIC

Está representado por el/la responsable del Área de Informática y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Contingencia Informático.
- Guiar y supervisar a los equipos operativos de contingencia informática, en el desarrollo de sus actividades.
- Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.
- Notificar y mantener informado al Secretario/a Técnico/a del EMED (Espacios de Monitoreo de Emergencias y Desastres) acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan, quien a su vez informará al Grupo de Trabajo de Gestión del Riesgo de Desastres del Hospital. En segunda instancia, se notificará y mantendrá informada a la jefatura de la Unidad de Estadística e Informática.

- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información y Comunicaciones (TIC) en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia Informático, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización de su impacto en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicaciones, en el menor tiempo posible.

El responsable del Equipo de Prevención de TIC es el/la Especialista en Seguridad de la Información.

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

b.1 Especialista en Seguridad de la Información

- Establecer y supervisar los procedimientos de seguridad de los servicios informáticos.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de desastres.
- Verificar la realización del mantenimiento preventivo a los equipos componentes del centro de datos y cuartos de comunicaciones.
- Verificar las tareas de copias de respaldo (backup).

b.2 Especialista en Redes y Comunicaciones

- Mantener actualizado el inventario hardware y software utilizado en el centro de datos y cuartos de comunicaciones.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del centro de datos y

cuartos de comunicaciones, considerando el tiempo de vida útil y garantía de los mismos.

- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del centro de datos y cuartos de comunicaciones.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del centro de datos y cuartos de comunicaciones.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación.

b.3 Técnico en Telecomunicaciones

- Monitorear el funcionamiento de la central telefónica.
- Verificar que la central telefónica cuenta con el soporte técnico.
- Mantener actualizada la lista de anexos telefónicos y de aquellos con acceso directo.
- Actualizar el software que utiliza la central telefónica.

ÁREA DE INFORMÁTICA HRM

b.4 Coordinador en Sistemas de Información

- Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida de software.
- Llevar un control de versiones de las fuentes de los sistemas de información y portal web.
- Coordinar y verificar que se realicen las copias de respaldo de las fuentes de los aplicativos informáticos existentes en un ambiente adecuado.

b.5 Especialista en Sistemas de Información

- Soporte y mantenimiento de los sistemas y aplicativos instalados en el hospital.
- Documentación, consolidación y validación de los manuales de los sistemas en producción.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.

b.6 Especialista en Administración de Base de Datos

- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de información.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas de información.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Seguridad de la Información.

c. Equipo de Emergencia de TIC

Este equipo es el encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información del hospital, procurando salvaguardar su pérdida o deterioro.

A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

ÁREA DE INFORMÁTICA HRM

c.1 Especialista en Redes y Comunicaciones

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en el Centro de Datos y cuartos de comunicaciones.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos y cuartos de comunicaciones, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

c.2 Técnico en Telecomunicaciones

- Ejecutar las acciones de emergencia en la central telefónica instalada en el Centro de Datos y el sistema de comunicación por radio comunicación VHF/HF del hospital
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

c.3 Coordinador en Sistemas de Información

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.

c.4 Especialista en Sistemas de Información

- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los "logs" de los aplicativos informáticos y sistemas de información afectados durante la emergencia.

c.5 Especialista en Administración de Base de Datos

- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

c.6 Técnico de Soporte Informático

- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios del hospital.

c.7 Especialista en Seguridad de la Información

- Apoyar en las labores de verificación y validación de operación de los servicios informáticos.

d. <u>Equipo de Restauración de TIC</u>

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir, en el menor tiempo posible, el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos del hospital de manera coordinada con el Grupo de Trabajo de Gestión del Riesgo de Desastres del hospital.

d.1 Especialista en Redes y Comunicaciones

- Es el responsable del equipo de Restauración de TIC

- Debe iniciar el proceso de recuperación de los servicios informáticos, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios informáticos y los equipos componentes del Centro de Datos del hospital.
- Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.

d.2 Técnico en Telecomunicaciones

- Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el Centro de Datos del hospital, así como de los anexos telefónicos.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los anexos y central telefónica ubicada en el Centro de Datos.

d.3 Coordinador en Sistemas de Información

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información y aplicativos informáticos.
- Coordinar y monitorear la restauración de sistemas de información y aplicativos, con la ejecución de pruebas para verificación su funcionalidad.

d.4 Especialista en Sistemas de Información

- Verificar el estado de los aplicativos alojados en los servidores de aplicaciones del hospital.
- En caso se requiera, desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.

- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información del hospital.

d.5 Especialista en Administración de Base de Datos

- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del hospital luego de efectuado el proceso de recuperación.

d.6 Técnico de Soporte

- Verificar el funcionamiento de los equipos personales en las áreas asistenciales y administrativas del hospital, distribuyendo el trabajo entre el personal técnico del Área de Informática.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del personal del hospital, luego de efectuado el proceso de recuperación.

d.7 Especialista en Seguridad de la Información

- Supervisar la restauración de los servicios informáticos.
- Validar la información documentada de los procedimientos de restauración utilizados.

Se debe considerar que el Equipo de Emergencia de TIC y el Equipo de Restauración de TIC podrían ejecutar sus actividades de forma paralela, de acuerdo al siguiente orden de operación:

Figura N° 02: Flujo del orden de operación de los equipos de TIC

8.3.2 FASE 2: DETERMINACIÓN DE VULNERABILIDADES Y ESCENARIOS DE CONTINGENCIA

En esta fase se procederá a la identificación de los recursos críticos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

8.3.2.1 Procesos institucionales

Para garantizar la continuidad de las actividades asistenciales y administrativas del Hospital Regional de Moquegua se busca la continuidad de los siguientes procesos, los cuales están ligados a los objetivos institucionales:

a) Atención integral de los servicios de salud a la población.
b) Gestión de riesgos para garantizar la seguridad físico funcional de los servicios de salud públicos.

8.3.2.2 Recursos críticos

A continuación, se detallan los procesos, aplicaciones y recursos críticos, con su respectiva expectativa máxima del tiempo de recuperación; así mismo, se hace una primera evaluación de sus niveles de criticidad para las operaciones internas y servicios externos del hospital, en torno a una variable ordinal con valores que representan una categoría a la cual se le ha asignado tres valores (alta, media, baja):

Tabla N° 01: Aplicaciones y/o Recursos Críticos de TIC

Procesos	Aplicaciones y/o Recursos Críticos	Tiempo de Recuperación Estimado (TRE)	Crítico para operaciones internas	Crítico para servicios externos
Gestión de redes e infraestructura de TIC	Equipos de comunicaciones.	12 hrs.	Alta	Media
	Equipos de protección eléctrica del centro de datos (UPS)	12 hrs.	Alta	Baja
	Sistema de aire acondicionado del Centro de Datos y Cuartos de comunicaciones	24 hrs.	Media	Baja
	Infraestructura del Centro de Datos	72 hrs.	Alta	Baja
	Sistema de Cableado Estructurado	24 hrs.	Alta	Baja
	Enlaces de cobre y fibra óptica para interconexión con el Centro de Datos	08 hrs.	Alta	Baja
	Sistema de Almacenamiento de la Información (storage)	12 hrs.	Media	Baja
	Medios de respaldo (cintas de backup)	08 hrs.	Alta	Baja
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	12 hrs.	Alta	Baja
	Servidores de red en general	12 hrs.	Alta	Baja
	Sistema de Central Telefónica IP	24 hrs.	Baja	Alta
Gestión de sistemas de información y bases de datos	Sistema de Conectividad y Seguridad Informática	08 hrs.	Alta	Baja
	Sistemas de información administrativos y portal web	48 hrs.	Media	Baja
	Sistemas de información asistenciales	24 hrs.	Alta	Baja
	Sistema de alarma contra incendios	12 hrs.	Media	Baja
	Sistema de Videovigilancia	12 hrs.	Media	Baja
	Sistema RIS/PAC	08 hrs.	Alta	Baja
	Sistema de Llamada de Enfermeras	12 hrs.	Media	Baja
	Sistema de Control de Energía (BMS)	12 hrs.	Media	Baja
	Sistema de Red Inalámbrica	12 hrs.	Baja	Baja
	Base de datos y repositorios utilizados por los sistemas y aplicaciones.	24 hrs.	Alta	Baja
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles, entre otros)	48 hrs.	Media	Baja
Operación y mantenimiento de TIC	Sistema de Comunicación VHF/HF	08 hrs.	Media	Media
	Sistema de Sonido Ambiental y Perifoneo	08 hrs.	Media	Baja
	Personal crítico responsable de los procesos de TIC.	04 hrs.	Alta	Baja

Nota: El TRE (Tiempo de Recuperación Estimado), ha sido determinado por el equipo de ingeniería del Área de Informática.

AREA DE INFORMÁTICA HRM

8.3.2.3 Priorización de restauración de servicios de TIC

La priorización para la restauración de los servicios de Tecnologías de Información y Comunicaciones se realizará según la siguiente tabla:

Descripción	Prioridad de Recuperación
Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos e internos y manejen alto volumen de información. Ejemplo: Sistema de Gestión Hospitalaria – SISGALENPLUS, servidores de bases de datos, entre otros.	1
Atención estándar: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistema de Información de Administrativo Financiera (SIAF), Sistema de Gestión Administrativa (SIGA), portal web institucional, Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.	2
Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Así mismo equipos de apoyo. Ejemplo: Intranet, entre otros.	3

Considerando la criticidad, se procederá a la restauración de las aplicaciones y/o recursos críticos de TIC según la siguiente prioridad

Tabla N° 02: Priorización de restauración de servicios de TIC

Aplicaciones y/o Recursos Críticos	Prioridad
Equipos de comunicaciones.	1
Equipos de protección eléctrica del centro de datos (UPS)	2
Sistema de aire acondicionado del Centro de Datos y Cuartos de comunicaciones	2
Infraestructura del Centro de Datos	1
Sistema de Cableado Estructurado	2
Enlaces de cobre y fibra óptica para interconexión con el Centro de Datos	1
Sistema de Almacenamiento de la Información (storage)	2
Medios de respaldo (cintas de backup)	2
Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	1
Servidores de red en general	1
Sistema de Central Telefónica IP	3
Sistema de Conectividad y Seguridad Informática	2
Sistemas de información administrativos y portal web	2
Sistemas de información asistenciales	1
Sistema de alarma contra incendios	3
Sistema de Videovigilancia	2
Sistema RIS/PAC	1
Sistema de Llamada de Enfermeras	3
Sistema de Control de Energía (BMS)	3
Sistema de Red Inalámbrica	3
Base de datos y repositorios utilizados por los sistemas y aplicaciones.	1

Aplicaciones y/o Recursos Críticos	Prioridad
Estaciones de trabajo del personal crítico (computadoras personales y portátiles, entre otros)	1
Sistema de Comunicación VHF/HF	3
Sistema de Sonido Ambiental y Perifoneo	3

8.3.2.4 Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios informáticos del hospital, considerando la ubicación geográfica, el contexto actual del hospital y su centro de datos.

Tabla N° 03: Amenazas a los servicios de TIC

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en el Centro de Datos.	
03	Falla en telecomunicaciones.	Tecnológicos
04	Delito informático.	
05	Falla de hardware y software.	
06	Incendio en el Centro de Datos.	Físico y ambiental
07	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicaciones.	
08	Ausencia o no disponibilidad del personal crítico de TIC.	Humanos
09	Pandemia y/o Epidemia	Ambiental

8.3.2.5 Probabilidad de ocurrencia

Es la cuantificación de que ocurra una amenaza realmente. Para el cálculo de probabilidad se utiliza la siguiente escala:

Probabilidad	Valor	Descripción
Baja	4	Se puede presentar al menos una vez en 5 años o más
Media	6	Se puede presentar al menos una vez en 3 años
Alta	8	Se puede presentar al menos una vez al año
Muy Alta	10	Se puede presentar más de 1 vez al año

Determinadas las amenazas que pueden afectar los recursos críticos de TIC, se calcula el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos. A continuación, se detalla el resultado obtenido:

Tabla N° 04: Probabilidad estimada de las amenazas a los servicios de TIC

N°	Amenaza (Evento)	Probabilidad de ocurrencia
01	Terremoto.	4
02	Inundación y aniego en el Centro de Datos.	4
03	Falla en telecomunicaciones.	10
04	Delitos informáticos.	4
05	Falla del hardware y software.	8
06	Incendio en el Centro de Datos.	4
07	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicaciones.	4
08	Ausencia o no disponibilidad del personal crítico de TIC.	4
09	Pandemia y/o Epidemia	6

8.3.2.6 Identificación de impacto

Permite calificar el nivel de afectación de la amenaza en caso de producirse. La medición puede ser cualitativa o cuantitativa.

En el presente plan la clasificación del impacto está hecha en base a una escala de 4 al 10, desde los niveles Baja hasta Muy Alta, como se muestra en la siguiente tabla:

Impacto	Valor	Descripción
Baja	4	No representa un impacto importante. Se cuenta con controles suficientes que responden a un programa de mantenimiento, se evidencia que han respondido a eventos ocurridos y ejercicios realizados, se puede prescindir del servicio por un tiempo limitado.
Media	6	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
Alta	8	Impacta en forma grave a un área o servicio específico, se puede llegar a comprometer información clasificada como confidencial, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto se limita dentro del Hospital Regional de Moquegua.
Muy Alta	10	Impacta en forma severa a todo el Hospital Regional de Moquegua y su efecto no solo se limita a éste. Compromete la confidencialidad o integridad de información crítica o la continuidad de las operaciones por paralización de los servicios más allá de los tiempos tolerables.

8.3.2.7 Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TIC del hospital frente a cada amenaza.

- Los ambientes del Área de Informática, denominado soporte informático, donde se ubica la central de comunicaciones, centro de datos y sala de

UPS que respalda a este último, se encuentran sobre el sistema de aisladores sísmicos instalados en la infraestructura del hospital.

- Cámaras de vigilancia en el interior y exterior del Centro de Datos.
- Equipo de seguridad perimetral (Firewall), renovado el año 2022, debidamente licenciado por el período de DOS (02) años.
- Grupo electrógeno y UPS dedicados que dan respaldo de energía eléctrica al centro de datos.
- Sistema de control de acceso al Centro de Datos y cuartos de comunicaciones.
- Respaldo de información en cintas almacenadas en el Centro de Datos.
- Uso de conexiones remotas seguras con VPN.
- Mantenimiento de generadores eléctricos y UPS. El mantenimiento de generadores (grupo electrógeno) y UPS está a cargo de la Unidad de Servicios Generales y Mantenimiento.
- Mantenimiento para equipos de aire acondicionado del Centro de Datos y cuartos de comunicaciones. El mantenimiento está a cargo de la Unidad de Servicios Generales y Mantenimiento.
- Redundancia en los enlaces de comunicaciones (fibra óptica).
- Sistema contra incendios en el Centro de Datos y su sala de UPS.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus, con licencia vigente y renovada anualmente, instalada en los servidores de red y computadoras.
- Solución de protección de portal web y aplicaciones web publicadas en internet a través de solución en la nube.
- Solución de correo electrónico en la nube.

AREA DE INFORMÁTICA HRM

8.3.2.8 Cálculo del Nivel de Riesgo

Se ha considerado los controles existentes que mitigan la afectación de las amenazas y/o el impacto descritas en el punto anterior. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Ocurrencia	Muy Alta	10	40 (Medio)	60 (Alto)	80 (Muy Alto)	100 (Muy Alto)
	Alta	8	32 (Medio)	48 (Alto)	64 (Alto)	80 (Muy Alto)
	Media	6	24 (Bajo)	36 (Medio)	48 (Alto)	60 (Alto)
	Baja	4	16 (Bajo)	24 (Bajo)	32 (Medio)	40 (Medio)
NIVEL DE RIESGO (probabilidad de ocurrencia x impacto)			4	6	8	10
			Bajo	Medio	Alto	Muy Alto
			Impacto			

A continuación, se tiene la interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Probabilidad	Descripción
Muy Alto	Riesgo no aceptable, se requiere acción correctiva inmediata.
Alto	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos.
Medio	Riesgo aceptable con revisión de la jefatura de la UEI, y se evalúa tomar acciones.
Bajo	Riesgo aceptable, sin revisión y no se requieren acciones.

Tabla N° 05: Resultado de la evaluación de riesgos de los servicios de TIC

ITEM	Amenazas (Eventos) / Recursos Críticos	↓ Impacto	Terremoto/Sismo	Inundación y aniego en el Centro de Datos.	Falla en telecomunicaciones.	Delito informático.	Falla de hardware y software.	Incendio en el Centro de Datos.	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicaciones.	Ausencia o no disponibilidad del personal crítico de TIC.	Pandemia y/o Epidemia
	Probabilidad de ocurrencia →		4	4	10	4	8	4	4	4	6
01	Equipos de comunicaciones.	10									
02	Equipos de protección eléctrica del centro de datos (UPS)	10									
03	Sistema de aire acondicionado del Centro de Datos y Cuartos de comunicaciones	8									
04	Infraestructura del Centro de Datos	10									
05	Sistema de Cableado Estructurado	8									
06	Enlaces de cobre y fibra óptica para interconexión con el Centro de Datos	10									
07	Sistema de Almacenamiento de la Información (storage)	8									
08	Medios de respaldo (cintas de backup)	6									
09	Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	8									
10	Servidores de red en general	6									
11	Sistema de Central Telefónica IP	6									
12	Sistema de Conectividad y Seguridad Informática	8									
13	Sistemas de información administrativos y portal web	6									
14	Sistemas de información asistenciales	8									
15	Sistema de alarma contra incendios	8									
16	Sistema de Videovigilancia	4									

ITEM	Amenazas (Eventos) / Recursos Críticos	Impacto	Terremoto/Sismo	Inundación y aniego en el Centro de Datos.	Falla en telecomunicaciones.	Delito informático.	Falla de hardware y software.	Incendio en el Centro de Datos.	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicaciones	Ausencia o no disponibilidad del personal crítico de TIC.	Pandemia y/o Epidemia
	Probabilidad de ocurrencia →		4	4	10	4	8	4	4	4	6
17	Sistema RIS/PAC	8									
18	Sistema de Llamada de Enfermeras	4									
19	Sistema de Control de Energía (BMS)	4									
20	Sistema de Red Inalámbrica	4									
21	Base de datos y repositorios utilizados por los sistemas y aplicaciones.	8									
22	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	4									
23	Sistema de Comunicación VHF/HF	6									
24	Sistema de Sonido Ambiental y Perifoneo	4									
25	Personal crítico responsable de los procesos de TIC.	6									

ÁREA DE INFORMÁTICA HRM

8.3.2.9 Escenarios de riesgo

A continuación, luego de la evaluación de riesgos se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Tabla N° 06: Escenarios de Riesgos

Item	Escenario de Riesgo	Descripción	Impacto
01	Interrupción de comunicaciones por problemas técnicos en servicios de internet y/o telefonía.	Consiste en el corte o interrupción de los servicios informáticos que utilizan el servicio de internet y/o telefonía, ocasionando pérdidas de comunicación en los equipos de la infraestructura tecnológica.	Alta
02	Indisponibilidad de los servidores de red y eventualmente de los equipos de cómputo por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, así como de equipos de cómputo, lo cual produce que la información o servicios brindados por los servidores no estén disponibles y/o que los usuarios finales no puedan acceder a los mismos.	Alta
03	Limitada capacidad de atención y gestión de los servicios informáticos	Este escenario consiste en el limitado número de personal del Área de Informática, en forma presencial, para la atención y gestión de los servicios	Media

Item	Escenario de Riesgo	Descripción	Impacto
	durante la declaratoria de una pandemia y/o epidemia.	informáticos y telecomunicaciones dadas las restricciones que se disponen a consecuencia de la declaratoria de una pandemia y/o epidemia.	

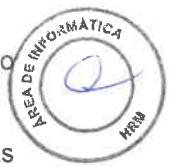
8.3.3 FASE 3: ESTRATEGIAS DEL PLAN DE CONTINGENCIA INFORMÁTICO

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre.

8.3.3.1 Estrategias de prevención de tecnologías de la información

a) Almacenamiento y respaldo de la información (BACKUPS)

- Gestión de copias de respaldo (Backup) de la información almacenada y procesada en el Centro de Datos, considerando la criticidad de los datos, la frecuencia de las tareas de backup, resguardo y transporte al sitio externo.
- Realizar copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.
- Se utiliza lugares alternativos externos para el almacenamiento de las copias de respaldo.



b) Sitios Alternos para el Centro de Datos

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Propios de la entidad.

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

c) Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos informáticos, con sus datos de contacto actualizados.

- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

d) Entrenamiento y personal de reemplazo

- Todo el personal del Área de Informática, debe entrenarse en el proceso de recuperación de los servicios informáticos. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos.
- Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes especialidades y procesos del Área de Informática, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
- Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica

- Programación de una revisión anual de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
- Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro adquirir equipos de reemplazo y contingencia.

f) Activación de trabajo remoto

- Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios informáticos.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la sede del hospital, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Administración.

- Realizar el trámite de certificados digitales, para instalarlos en los equipos de los usuarios, fuera de la institución.
- Activación del desvío de las llamadas telefónicas a los usuarios asignados encargados de la atención de la central telefónica.
- Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios informáticos, a cargo del Área de Informática en el Centro de Datos.

8.3.3.2 Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del hospital y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre. A continuación, se citan las acciones que se realizarán durante una contingencia:

Acciones durante la contingencia:

- Evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
- Informar al responsable del Grupo de Trabajo de Gestión del Riesgo de Desastres del hospital sobre la situación presentada, para decidir la realización de la declaración de contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

8.3.3.3 Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos del hospital para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo

cual se definen las pautas que permitan al personal del Área de Informática garantizar la continuidad de las operaciones en el hospital.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Figura N° 03: Ciclo de la estrategia de recuperación de TIC

La priorización de la restauración de los servicios de tecnologías de información y comunicaciones del hospital se ejecutará de acuerdo a lo indicado en la Tabla N° 02.

En el Anexo 01 y 02 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

Acciones después de la contingencia:

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia Informático.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

8.3.4 FASE 4: ELABORACIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los planes de contingencia agrupados por las categorías indicadas previamente.

El Plan de Contingencia Informático comprenderá los eventos de mayor impacto, identificados en la matriz de evaluación de riesgos (Tabla N° 05), los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 07: Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Falla en telecomunicaciones	Muy Alto	FPC – 01
2	Falla de hardware y software	Muy Alto	FPC – 02
3	Pandemia y/o Epidemia	Alto	FPC – 03

En el Anexo N° 03 se presenta el desarrollo de cada formato.

8.3.5 FASE 5: DEFINICIÓN Y EJECUCIÓN DEL PLAN DE PRUEBAS

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos del Área de Informática, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- Metodología (descripción de la prueba a efectuarse)
- Alcances (áreas afectadas / personal involucrado)
- Resultados

Las pruebas relacionadas a este plan, se deberán ejecutar cada cuatro (04) meses, para el caso en agosto y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado del Anexo N° 04.

8.3.6 FASE 6: IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO

La implementación del presente plan se realizará a partir de su aprobación mediante acto resolutivo.

Para tal efecto, el/la responsable del Área de Informática, realiza las siguientes funciones:

- Supervisar las actividades de copias de respaldo y restauración.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información y Comunicaciones (TIC).
- Participar en las pruebas y simulacros de desastres.

8.3.7 FASE 7: MONITOREO

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

- Realizar mantenimiento de la documentación técnica de operación de los servicios informáticos.
- Revisión continua de los aplicativos, sistemas de información y portal web.
- Revisión continua del sistema de copias de respaldo (backups).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos, para esto se coordinará con la Unidad de Servicios Generales y Mantenimiento

IX. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD PREVENTIVAS	MES 2023						
		JUN	JUL	AGO	SET	OCT	NOV	DIC
01	Socialización del Plan de Contingencia Informática con el personal del Área de Informática y asignación de roles, funciones y responsabilidades dentro del Plan	X						
02	Implementación del Plan de Contingencia Informática	X	X	X	X	X	X	X
03	Simulacro – Ejecución del Plan de Pruebas			X				X
04	Realizar el inventario hardware y software utilizado en el Centro de Datos y Cuartos de comunicaciones	X						
05	Ejecutar copias de respaldo (backup)	X	X	X	X	X	X	X
06	Mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos					X	X	
07	Mantenimiento preventivo de los computadores personales, laptops, equipos de impresión, UPS	X			X	X	X	
08	Revisión de obsolescencia tecnológica en los equipos de comunicaciones y de los equipos componentes del Centro de Datos					X	X	

N°	ACTIVIDAD PREVENTIVAS	MES 2023						
		JUN	JUL	AGO	SET	OCT	NOV	DIC
09	Revisión de obsolescencia tecnológica en los computadores personales, laptops, equipos de impresión, UPS	X			X	X	X	
10	Actualizar la lista de anexos telefónicos		X					
11	Actualizar licencia de solución antivirus					X		
12	Actualizar firmware y/o licencia de equipo de seguridad perimetral	X						X

Nota: Las actividades 06 y 07 serán ejecutadas en cumplimiento a sus respectivos planes aprobados

X. COSTO DEL PLAN

Para la implementación del presente plan se requiere contar con la disponibilidad presupuestal detallada en los siguientes ítems:

Recursos Económicos de Funcionamiento del Hospital (Personal y Bienes)

PERSONAL			
Tipo de Personal	**Cantidad**	**Costo Unitario Aproximado (S/)**	**Costo Total Aproximado (S/)**
Ingeniero de Sistemas / Informático	04	0.00	0.00
Técnico en Computación / Informática	04	0.00	0.00
TOTAL			0.00

El hospital cuenta con el personal requerido para la ejecución de las actividades del presente plan, son técnicos y profesionales especializados en informática y sistemas de información; razón por la cual no representará un costo adicional para la institución.

BIENES			
Tipo de Personal	**Cantidad**	**Costo Unitario Aproximado (S/)**	**Costo Total Aproximado (S/)**
Unidad portátil de intercomunicación	08	1,500.00	12,000.00
Cinta tape backup LTO 5/Ultrium 1.5/3 TB	10	250.00	2,500.00
TOTAL			14,500.00

Las unidades portátiles de intercomunicación, tienen el objetivo de implementar una vía de comunicación alterna, ante la caída del servicio de telefonía móvil y fija, a consecuencia de la ocurrencia de algún escenario de riesgo y la implementación de las actividades preventivas señaladas.

Las cintas tape backup, son el insumo necesario para respaldar la información de las bases de datos previamente identificadas, necesarias para la solución de copias de seguridad en cinta de gran capacidad, instalada en el centro de datos.

SERVICIOS			
Tipo de Personal	Cantidad	Costo Unitario Aproximado (S/)	Costo Total Aproximado (S/)
Línea de respaldo de internet	01	30,000.00	30,000.00
Líneas adicionales de telefonía móvil	03	900.00	2,700.00
TOTAL			32,700.00

La línea de respaldo de internet, es la propuesta para afrontar el evento de Falla en telecomunicaciones, desarrollado en el Anexo N° 03 (FPC – 01); el costo total aproximado, involucra el período de un año.

Las líneas adicionales de telefonía móvil, es parte de la alternativa planteada para hacer frente el evento de Pandemia y/o Epidemia, detallado en el Anexo N° 03 (FPC – 03), situación particular experimentada en la pandemia por el COVID-19, en las que se hace necesario la atención de las necesidades por los servicios informáticos, incluso fuera de la jornada laboral, a través de telefonía móvil con acceso a datos, sin que se tenga que recurrir a equipos de uso personal, con la capacidad de acceder a aplicaciones de acceso remoto y conectividad a redes VPN. Su costo aproximado incluye la adquisición del equipo y el pago por el servicio durante el período de 12 meses.

ÁREA DE INFORMÁTICA HRM

Recursos Económicos a ser priorizados por el Hospital que implica adquisición:

A continuación, se detalla el presupuesto necesario para la implementación de las actividades en las que se requiere los bienes y servicios señalados:

Específica de Gasto	Monto	Meta SIAF	Fuente de Financiamiento
2.3. 1 6. 1 2	12,000.00	81	Recursos Ordinarios
2.3. 1 5. 1 2	2,500.00	81	Recursos Ordinarios
2.3. 2 2. 2 3	30,000.00	81	Recursos Ordinarios
2.3. 2 2. 2 1	2,700.00	81	Recursos Ordinarios
TOTAL	47,200.00		

XI. ANEXOS

ANEXO 01

LISTADO DE APLICATIVOS Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema / Aplicación	Breve descripción	Área Usuaria	Tipo	Prioridad
1	SISGALEN	Sistema de Gestión Hospitalaria	Asistenciales y administrativas	Escritorio	1
2	SIAF	Sistema de Información de Administración Financiera	Personal, Presupuesto, Logística, Economía	Escritorio	1
3	SIGA	Sistema Informático de Gestión Administrativa	Asistenciales y administrativas	Escritorio	1
4	SISMED	Sistema de Gestión de Medicamentos e Insumos	Farmacia	Escritorio	1
5	RIS/PAC	Registro y administración de los estudios en el Servicio de Diagnóstico por Imágenes	Diagnóstico por Imágenes y asistenciales	Escritorio	1
6	HELPNEX	Sistema de Llamada de Enfermeras	Emergencia, Hospitalización, Centro Quirúrgico	Escritorio	2
7	Portal Web Institucional	Publicación de información institucional en páginas web	Asistenciales, administrativas y público en general	Web	2
8	AVIGILON	Sistema de gestión de video vigilancia.	Empresa externa contratada para su operación	Escritorio	2
9	BMATIC	Sistema de gestión de colas	Consulta Externa, Emergencia, Diagnóstico por Imágenes, Farmacia, Seguros	Web	1
10	BIOSTAR	Sistema de Control de Asistencia	Asistenciales y administrativas	Escritorio	2
11	Sistema de Control de Asistencia	Sistema complementario para la gestión de la información de BIOSTAR y programación de turnos	Asistenciales y administrativas	Escritorio	2
12	SIAT	Aplicación para el registro de información para apoyo al tratamiento y el diagnóstico.	Laboratorio, Diagnóstico por Imágenes, Anatomía Patológica	Escritorio	2
13	Sistema de Control de Energía - BMS	Permite monitorear el funcionamiento de los equipos eléctricos y electromecánicos	Unidad de Servicios Generales y Mantenimiento	Escritorio	3
13	Sistema de Convocatorias CAS	Permite el registro de la postulación en línea de las convocatorias CAS	Unidad de Personal	Web	3
14	SFS - Sistema Facturador de la SUNAT	Envío de Información de Comprobantes Electrónicos a la SUNAT	Unidad de Economía	Web	3
15	SIEOC	Aplicación para el registro de Exámenes Ocupacionales	Consulta Externa	Escritorio	3
16	SIEMEL	Aplicación que genera información para la Facturación Electrónica a ser utilizada por el Facturador de la SUNAT	Unidad de Economía	Escritorio	3

ÁREA DE INFORMÁTICA HRM

ANEXO N° 02

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y CUARTOS DE COMUNICACIONES CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

CENTRO DE DATOS				
Cant.	**Tipo de Equipo**	**Rol**	**Descripción**	**Prioridad**
8	Servidor Blade	Aplicaciones	Equipo de almacenamiento de información, donde se configuran las máquinas virtuales.	1
1	Servidor (virtual)	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS).	1
1	Servidor (virtual)	Aplicaciones	Servidor FTP	3
1	Servidor	Base de Datos	Servidor que gestiona software AVIGILON del Sistema de Cámaras de Video vigilancia	2
1	Servidor	Base de Datos	Servidor que gestiona software CARESTREAM del Sistema de RIS PACS	1
1	Servidor	Telefonía	Servidor de la Central Telefónica IP	3
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de Control de Acceso	2
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de llamada de Enfermeras	2
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de Gestión de Colas	1
1	Servidor	Aplicaciones	Servidor del Sistema de Control de Energía - BMS	3
1	Servidor (virtual)	Aplicaciones	Servidor para Sistema de Gestión Hospitalaria (SISGALEN)	1
1	Servidor (virtual)	Aplicaciones	Servidor para Sistema Integrado de Gestión Administrativa (SIGA)	2
1	Servidor (virtual)	Aplicaciones	Servidor para el Sistema de Integrado de Administración Financiera (SIAF)	2
1	Servidor (virtual)	Aplicaciones	Servidor para el Aplicativo de Registro de Formatos del Seguro Integral de Salud (ARFSIS)	1
1	Servidor (virtual)	Aplicaciones	Servidor para la Consola Eset (Antivirus)	1
1	Equipo Firewall	Seguridad	Equipo FORTINET para gestionar políticas de seguridad	2
1	Equipo	Controlador de red	Equipo para el Sistema de Red Inalámbrica	3
1	Equipo	Reloj Patrón	Sistema de Relojes Sincronizados IP	3
1	Panel de Extinción	Seguridad	Sistema automático de extinción de incendios para el Centro de Datos	1

CUARTO DE COMUNICACIONES					
N °	**Ambiente**	**Tipo Equipo**	**Cant.**	**Descripción**	**Prioridad**
1	GDS101	Switch de Borde	5	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
2	GDS102	Switch de Borde	3	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
3	GDS103	Switch de Borde	3	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
4	GDS104	Switch de Borde	1	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1

ÁREA DE INFORMÁTICA HRM

CUARTO DE COMUNICACIONES					
N °	Ambiente	Tipo Equipo	Cant.	Descripción	Prioridad
		UPS	1	Fuente de poder ininterrumpida	1
5	GDS105	Switch de Borde	1	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
6	GDS106	Switch de Borde	3	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
7	GDS201	Switch de Borde	3	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
8	GDS202	Switch de Borde	4	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
9	GDS203	Switch de Borde	3	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
10	GDS204	Switch de Borde	5	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
11	GDS301	Switch de Borde	4	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
12	GDS302	Switch de Borde	2	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
13	GDS401	Switch de Borde	4	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1
14	GDS402	Switch de Borde	2	Equipo de comunicación	1
		Equipo MCQuay	1	Equipo de aire acondicionado	1
		UPS	1	Fuente de poder ininterrumpida	1

ANEXO 03:

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO

HRM	EVENTO: Falla en telecomunicaciones	FPC – 01

1.PLAN DE PREVENCIÓN

a. Descripción del evento

Las telecomunicaciones constituyen un conjunto de técnicas que permiten la comunicación a distancia, es un recurso importante para el desarrollo de las actividades administrativas y asistenciales del hospital, dado que a través de su uso se logra la concreción de procesos y el acceso a fuentes de información que se encuentran fuera del hospital.

En ausencia de este, los sistemas de información que lo requieren no funcionan correctamente; por lo tanto, la parte afectada o causa de la contingencia, son los que a continuación se muestran:

Internet

- Permite la comunicación a distancia, compartir recursos y el acceso a una gran cantidad de información desde cualquier parte del mundo donde esté disponible la conectividad a dicho servicio.

Telefonía

- Acceso a comunicaciones de larga distancia relacionadas con la voz y mensajería de textos cortos (SMS).

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información.

b. Objetivo

Asegurar la continuidad de las comunicaciones a distancia, con el uso de los servicios de internet y telefonía.

c. Entorno

Se puede producir durante el servicio, afectando a los aplicativos y sistemas de información usados para dar soporte a las operaciones del Hospital

d. Personal Encargado

Equipo de Prevención de TIC.

e. Condiciones de Prevención de Riesgo

- Contratar una línea de respaldo del servicio de internet, con un ancho de banda mínimo, que garantice la continuidad del servicio.
- Identificación del equipo router, switch y fibra óptica instalados por la empresa proveedora del servicio de internet/telefonía en el centro de datos.

f. Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de telecomunicaciones.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos, asociados a las telecomunicaciones.

ÁREA DE INFORMÁTICA HRM

- Realizar monitoreo del funcionamiento de los equipos de telecomunicaciones instalados en el Centro de Datos y cuartos de comunicaciones, y verificar su estado tanto físicamente como a través de su plataforma monitor.
- Revisar diariamente del consumo de ancho de banda y el número de sesiones establecidas por el uso del servicio de internet, a fin de prevenir picos de saturación que ralenticen su acceso.
- Verificar los dispositivos enlazados a internet, en particular los que hacen uso de la red wifi.

2.PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b. Procesos Relacionados antes del evento

- Configuración de la línea de respaldo del servicio de internet en el equipo de seguridad perimetral.
- Disponibilidad de la lista de escalamiento para la solución de incidencias con el/los proveedor/es.

c. Personal que autoriza la contingencia

El/la Coordinador/a de Continuidad de TIC debe activar la contingencia.

d. Descripción de las actividades después de activar la contingencia

- Comunicarse con el proveedor del servicio afectado (internet o telefonía) para la solución de la incidencia.
- Verificar el funcionamiento de la línea de respaldo del servicio de internet.

e. Duración

El tiempo máximo de la contingencia no debe sobrepasar las seis (06) horas.

3.PLAN DE RECUPERACIÓN

a. Personal Encargado

El Equipo de Restauración de TIC, luego de validar la corrección del problema de comunicación informará a el/la Coordinador/a de Continuidad de TIC, quien comunicará a los jefes de áreas para el normal desarrollo de las operaciones en los servicios afectados.

b. Descripción de actividades

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio de telecomunicaciones.

Se debe realizar como mínimo las siguientes actividades:

- Verificar la operatividad de la línea de respaldo del servicio de internet.
- Establecer contacto con el proveedor del servicio afectado para recibir instrucciones inmediatas y/o ayuda para la recuperación del servicio.
- Supervisar el progreso de las operaciones de recuperación de los servicios de telecomunicaciones y mantener informado al Grupo de Trabajo de Gestión del Riesgo de Desastres.
- Restaurado el servicio, ejecutar pruebas de acceso y consumo de información que depende de los servicios de telecomunicación.

ÁREA DE INFORMÁTICA HRM

HRM	EVENTO: Falla en telecomunicaciones	FPC – 01

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c. Mecanismos de Comprobación

Se registrará el incidente en el Formato de Reporte de Incidentes de Mantenimiento Preventivo y/o Correctivo del Área de Informática, precisando las acciones realizadas.

El/la responsable del Equipo de Restauración de TIC, presentará un informe a el/la Coordinador/a de Continuidad de TIC, explicando que servicios u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d. Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC, se desactivará el presente Plan.

e. Proceso de Actualización

En base al informe presentado por el/la Coordinador/a de Continuidad de TIC, donde se identifica las causas de la interrupción o fallas en las telecomunicaciones, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el/la Especialista en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos.

ÁREA DE INFORMÁTICA HRM

HRM	EVENTO: Falla de hardware y software	FPC – 02

1.PLAN DE PREVENCIÓN

a. Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad. Los equipos de cómputo de los usuarios finales, es hardware y software necesario para el desarrollo de sus actividades y productividad.

En ausencia de estos, los sistemas de información no pueden funcionar, siendo la parte afectada o causa de la contingencia, los que se detallan a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Equipos de cómputo

Software

- Aplicaciones usadas por el Hospital y de servicio al ciudadano

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información.

ÁREA DE INFORMÁTICA HRM

b. Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de las imágenes de los servidores o máquinas virtuales en producción; así mismo, con la provisión de equipos de cómputo de contingencia para los usuarios finales.

c. Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del hospital

d. Personal Encargado

Equipo de Prevención de TIC.

e. Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de la entidad, así como de las imágenes de los servidores.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.
- Disponer de servidores de Aplicaciones de contingencia.
- Disponer de equipos de cómputo de contingencia.

f. Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.

HRM	EVENTO: Falla de hardware y software	FPC – 02

- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos y equipos de cómputo en general.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual; así como de los equipos de cómputo en general.

2.PLAN DE EJECUCIÓN

f. Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

g. Procesos Relacionados antes del evento

- Disponibilidad de las copias de respaldo.
- Disponibilidad de instaladores de sistemas operativos y motor de base de datos.
- Disponibilidad de al menos un servidor físico de contingencia.
- Disponibilidad de equipos de cómputo de contingencia.

h. Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

i. Descripción de las actividades después de activar la contingencia

- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.
- Solicitar las copias de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.
- En el caso de equipos de cómputo, se reemplazará inmediatamente con un equipo de contingencia, con los aplicativos y sistemas de información necesarios.

j. Duración

El tiempo máximo de la contingencia no debe sobrepasar las cuatro (04) horas.

3.PLAN DE RECUPERACIÓN

f. Personal Encargado

El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores y los presentados en los equipos de cómputo en general, informará a el/la Coordinador/a de Continuidad de TIC, este último informará a los jefes de áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

g. Descripción de actividades

El plan de recuperación estará orientado a recuperar, en el menor tiempo posible, las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores y/o equipos de cómputo, para el caso de los usuarios finales.

ÁREA DE INFORMÁTICA HRM

Se debe realizar como mínimo las siguientes actividades:

- Instalación y puesta a punto de un equipo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.
- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios del hospital informando la reanudación de los servicios.

Para el caso de los equipos de cómputo, se ejecutará las actividades señaladas en el plan de mantenimiento de equipos informáticos.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

ÁREA DE INFORMÁTICA HRM

h. Mecanismos de Comprobación

Se registrará el incidente en el Formato de Reporte de Incidentes de Mantenimiento Preventivo y/o Correctivo del Área de Informática, precisando las acciones realizadas.

El/la responsable del Equipo de Restauración de TIC, presentará un informe a el/la Coordinador/a de Continuidad de TIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

i. Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC, se desactivará el presente Plan.

j. Proceso de Actualización

En base al informe presentado por el/la responsable del Equipo de Restauración de TIC, quien informa las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el/la responsable del Equipo de Restauración de TIC deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

HRM	EVENTO: Pandemia y/o Epidemia	FPC – 03

1.PLAN DE PREVENCIÓN

a. Descripción del evento

Limitada presencia física del personal del Área de Informática, para la atención y gestión de los servicios informáticos, durante la declaratoria de una pandemia y/o epidemia; hecho que se magnifica al ser el escenario un establecimiento de salud, que necesita de personal técnico y especializado para la atención de las necesidades informáticas.

b. Objetivo

Asegurar las capacidades de atención y gestión de los servicios informáticos por parte del personal del Área de Informática.

c. Entorno

Este evento puede darse en las áreas especializadas del Área de Informática, el Centro de Datos, cuartos de comunicaciones y cualquier área asistencial o administrativa donde se requiera o haga uso de servicios informáticos.

d. Personal Encargado

El Equipo de Prevención de TIC.

e. Condiciones de Prevención de Riesgo

- Programación de las vacaciones del personal durante el año a fin de que no se tenga un desabastecimiento del personal técnico y especializado.
- Garantizar la inmunización anual del personal del Área de Informática, acorde a su etapa de vida, en coordinación con el Área de Inmunizaciones – Consulta Externa.
- Disponibilidad de equipos de protección personal, en calidad y cantidad necesarias, para la protección del personal en su estancia y desplazamiento por las instalaciones del hospital.
- Instalación y configuración de software de asistencia remota en los equipo de cómputo para la asistencia de personal técnico y configuración de los accesos a los servidores a través de red VPN.
- Disponibilidad de equipos de cómputo como contingencia, que facilite los trabajos de mantenimiento correctivo.

f. Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de soporte, asistencia técnica y restauración de información de forma remota.
- Coordinar y supervisar el mantenimiento preventivo de los sistemas de comunicaciones, equipos de cómputo, equipamiento del centro de datos, cuartos de comunicaciones y todos los elementos de la infraestructura tecnológica.
- Definir herramientas tecnológicas que permitan la continuidad de las labores especializadas del equipo de ingeniería en el desarrollo y mantenimiento de los aplicativos y sistemas de información, en forma remota.

2.PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Declaratoria de emergencia sanitaria a causa de una pandemia y/o epidemia, que limite la asistencia presencial del personal del Área de Informática en el hospital.

ÁREA DE INFORMÁTICA HRM

b. Procesos Relacionados antes del evento

- Actividades que requieran de asistencia y soporte informático dentro de las instalaciones.
- Disponibilidad de la lista de equipos de cómputo con sus credenciales de acceso al software para asistencia remota.

c. Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

d. Descripción de las actividades después de activar la contingencia

- Comunicar a todo el personal del Área de Informática sobre la activación de la contingencia.
- Comunicar a todos los servicios del hospital los números telefónicos institucionales (se considera el equipo actual asignado a la responsable del Área de Informática y los tres adicionales planteados en el presente plan para el personal de ingeniería) y anexos del personal informático para la atención de requerimientos por asistencia y soporte.
- Elaborar un rol para la asistencia y soporte técnico, en forma presencial, del mínimo personal técnico y especializado.
- Activación de los accesos a los servidores por red VPN.

e. Duración

El tiempo máximo de duración de la contingencia dependerá del término de la declaratoria de emergencia por parte de la máxima autoridad en salud (MINSA).

ÁREA DE INFORMÁTICA HRM

3.PLAN DE RECUPERACIÓN

a. Personal Encargado

El Equipo de Restauración de TIC, son quienes se encargarán de realizar las acciones de recuperación necesarias.

b. Descripción de actividades

El evento será evaluado y se debe realizar como mínimo las siguientes actividades:

- Al retorno a la presencialidad, hacer una evaluación del estado de los equipos tecnológicos en el centro de datos, cuartos de comunicaciones y demás de la infraestructura tecnológica.
- Evaluación del estado de salud (físico y psicológico) del personal del Área de Informática, en coordinación con el área de salud ocupacional, para la ejecución de actividades en zonas aún críticas y el hospital en general.
- Identificar al personal que continuará haciendo teletrabajo.

c. Mecanismos de Comprobación

El/la responsable del equipo de Restauración de TIC presentará un informe a el/la Coordinador/a de Continuidad de TIC, explicando el estado de los servicio informáticos, equipos u operaciones de tecnología de la información y cuáles son las acciones correctivas y/o preventivas a realizar.

Este informe deberá ser elevado al Grupo de Trabajo de Gestión del Riesgo de Desastres del Hospital.

d. Desactivación del Plan de Contingencia

El/La Coordinador de Continuidad de TIC desactivará el Plan de Contingencia una vez que todo el personal de informática retorne al trabajo presencial.

HRM	EVENTO: Pandemia y/o Epidemia	FPC – 03

e. Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

ANEXO 04:

FORMATO DE CONTROL Y CERTIFICACIÓN DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA N° _____

Escenario de Prueba: *(Descripción del escenario a probar/certificar)*

Área Responsable: *(Área responsable del escenario de prueba a probar/certificar)*

INFORMACIÓN EL PROCESO

Metodología: *(Detallar lo que se va a hacer en la prueba)*

Alcance: *(Definir hasta donde va a abarcar)*

Condiciones de Ejecución:

Equipo: *Nombre Servidor/ PC de prueba*

Aplicación/Software:

Ubicación: *Lugar de Prueba*

Fecha de Backup: *dd/mm/aaaa*

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio ☐ Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones:

ACTUALIZACIÓN EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: *(Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)*

ACTUALIZACIÓN DE PARTICIPANTES

Participante	Cargo	Firma

ÁREA DE INFORMÁTICA

Ronald Z. Cuevas Machaca
INGENIERO DE SISTEMAS
CIP. 86445

Ruth M. Limache Melendez
ING. DE SISTEMAS E INFORMATICA
Reg. CIP. 133710

KATHERINE DE LOS MILAGROS ELÍAS QUISPE
ING. EN INFORMÁTICA Y SISTEMAS
Reg. CIP 165726

Sug. Milagros Stelman Uribe
ING. DE SISTEMAS
CIP. 106471