MOQUEGUA

Nº 258-2021-GERESA-HRM/DE

Resolución Ejecutiva Directoral

Moquegua, 21 de octubre de 2021

VISTOS: Informe N° 0165-2021-GERESA-HRM/074-0/INFORM del Área de Informática; Informe N° 306-2021-GERESA-HRM/07 de fecha 01 setiembre del 2021 de la Unidad de Estadística e Informática, Informe N° 428-2021-GERESA-HRM/05 de fecha 13 de octubre de 2021 emitido por Unidad de Gestión de Calidad del Hospital Regional de Moquegua;

CONSIDERANDO:

Que, mediante el Informe de visto, la Jefa de la Unidad de Estadística e Informática solicita la aprobación mediante acto resolutivo del "Plan de Contingencia Informático 2021 del Hospital Regional de Moquegua, en ese contexto con el fin de establecer medidas de protección de los sistemas y la información que se procesa y ante un evento adverso permitir la recuperación de las operaciones y las capacidades para procesar la información hospitalaria, así mismo permitirá levantar la observación hecha al respecto por la Sociedad Auditora;

Que, el artículo 9° de la Ley N° 29733, Ley de Protección de Datos Personales, establece que el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate;

Que, mediante Resolución Ministerial N° 520-2006/MINSA, del 30 de mayo de 2006, se aprobó el documento técnico "Lineamientos de Política de Seguridad de la Información del Ministerio de Salud", con el fin de preservar la integridad, disponibilidad y confidencialidad de la información del Ministerio de Salud, en todos sus medios de soporte y tratamiento;

Que, mediante Resolución Ministerial N° 246-2007-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a Edición" en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública;

Que, mediante Resolución Ministerial N° 431-2015/MINSA Aprueba el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud - MINSA", reconoce que, la información que genera y dispone es un activo que, como otros activos importantes, tiene valor para la institución y requiere, en consecuencia, una protección adecuada. En tal sentido, es importante implementar un compromiso con el desarrollo, el mantenimiento de sistemas de información y el tratamiento de información no automatizada. Asimismo, el Ministerio de Salud protege y defiende la salud de la población, como expresión del ejercicio de la Rectoría Sectorial, con pleno respeto del derecho de toda persona a la protección de sus datos personales de acuerdo a lo establecido por la Ley N° 29733, Ley de Protección de Datos Personales;

Que, por los motivos antes expuestos resulta procedente emitir el acto resolutivo respectivo y 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 1º.- Aprobar el "**Plan de Contingencia Informático del Hospital Regional de Moquegua 2021**" por las consideraciones expuestas, el cual consta de cincuenta y uno (51) folios y que en anexo adjunto forman parte integrante de la presente Resolución;

Artículo 2º.- Disponer a la Jefa de la Unidad de Estadística e Informática del Hospital Regional de Moquegua, adopte las acciones administrativas y asistenciales para el cumplimiento del Plan de Contingencia.

Artículo 3º.- Disponer que la presente Resolución Ejecutiva Directoral se publique en el portal institucional www.hospitalmoquegua.go.pe

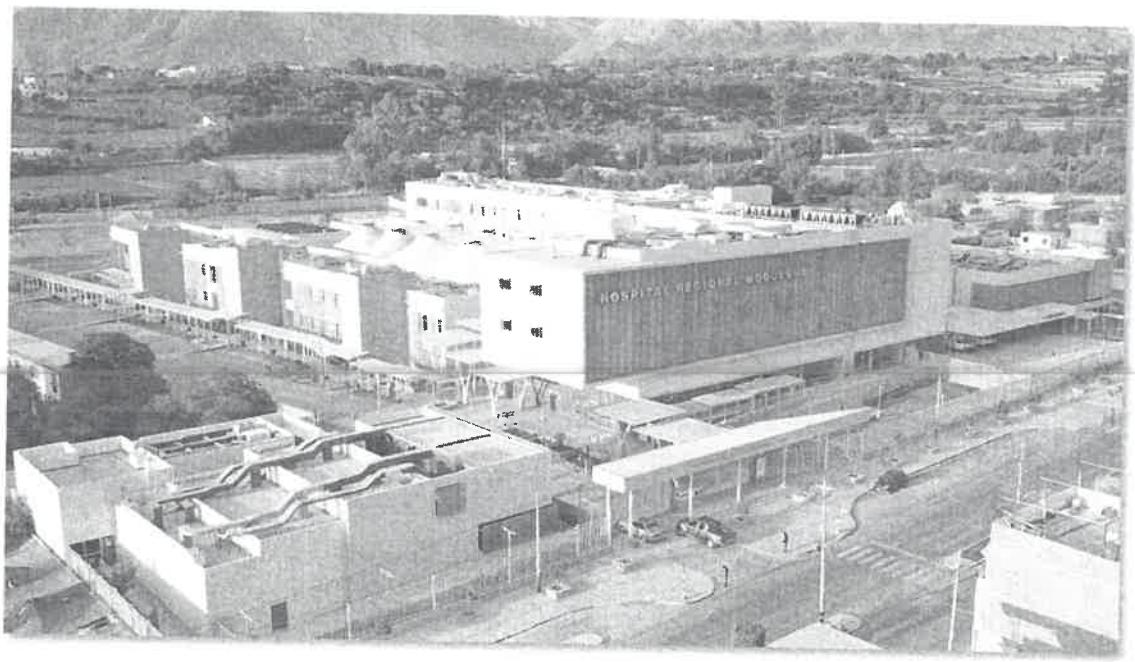
REGÍSTRESE Y COMUNÍQUESE

RFZC/DHRM
KOCHB/AL
C/C D. GENERAL
ADMINISTRACION
INFORMATICA
CALIDAD
ARCHIVO

HOSPITAL REGIONAL DE MOQUEGUA
DIRECCIÓN EJECUTIVA

HOSPITAL REGIONAL DE MOQUEGUA
M.E. RAÚL FORTUNATO ZEA CALCINA
CMP 34884 RNE 30316
DIRECTOR EJECUTIVO

PLAN DE CONTINGENCIA INFORMÁTICO



UNIDAD DE ESTADÍSTICA E INFORMÁTICA

AREA DE INFORMÁTICA

2021

CONTENIDO

PLAN DE CONTINGENCIA INFORMÁTICO - 2021

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), más aún desde el funcionamiento en su nueva sede (Noviembre-2019), la cual cuenta con 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 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 de las operaciones y las capacidades para procesar la información.

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 hospitalarios, ya sean asistenciales o administrativos, por algún inconveniente que pudiera presentarse con los mismos.

1.1 BASE LEGAL

- Ley N° 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 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.

III. FINALIDAD

Tener un Plan de Contingencia lo más objetivo e integral posible, 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 a los usuarios externos e internos 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 y restablecer el normal funcionamiento del 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	Cuevas Machaca Ronald Zenón	Ingeniero de Sistemas	rzcuevasm@hospitalmoquegua.gob.pe	953707292
02	Elías Quispe Katherine De los Milagros	Ingeniero de Sistemas	kelias@hospitalmoquegua.gob.pe	950269607
03	Limache Melendez Ruth Mariela	Ingeniero de Sistemas	rlimache@hospitalmoquegua.gob.pe	939132424
04	Stelman Uribe Suge Milagros	Ingeniero de Sistemas	sstelman@hospitalmoquegua.gob.pe	945698767

VI. CARACTERIZACIÓN DEL PLAN

6.1 DEFINICIONES

Plan de Contingencia Informático: Es un documento que reúne 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 organización.

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.

Incidente: Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. 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.

En el Anexo 1, se detalla la metodología utilizada en el presente Plan.

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.

6.2 METODOLOGIA

El desarrollo del presente Plan seguirá la siguiente metodología basada en siete (7) fases:

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

A continuación, se detalla cada fase:

6.2.1 FASE 1: PLANIFICACIÓN

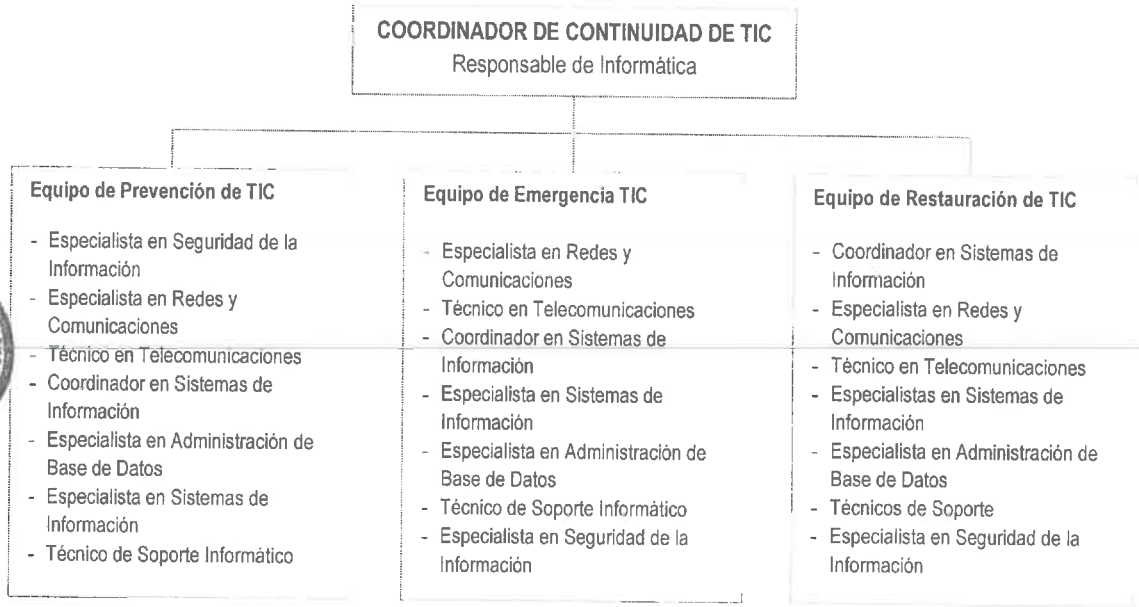
6.2.1.1 Organización

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 informáticos 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 y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal del Área de Informática.

Figura N° 1: Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones (TIC)



La jefatura de la Unidad de Estadística e Informática, a propuesta del Responsable de Informática, designa un miembro titular y un alterno, por cada integrante de los TRES (03) equipos mencionados previamente, detallados en la Figura N° 1. Para tal efecto, se debe contar con la relación del personal del Área de Informática que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

Asimismo, el Responsable de Informática debe tener operativo el dispositivo móvil asignado por el hospital para las comunicaciones pertinentes. Así mismo, la relación del personal del Área de Informática que forma parte del Plan de Contingencia debe ser actualizada 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.
- Casetas de vigilancia.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en 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.

6.2.1.2 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 y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

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 y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.
- 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.

- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) 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 y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, 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:

Especialista en Seguridad de la Información

- Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
- 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.
- Verificar las tareas de copias de respaldo (backup).

Especialista en Redes y Comunicaciones

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.

- 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, 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.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- 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.

Técnico en Telecomunicaciones

- Monitorear el funcionamiento de la Central Telefónica
- Verificar que la central telefónica cuenta con las garantías requeridas.
- Mantener actualizada la lista de anexos y teléfonos.
- Actualizar el software que utiliza la central telefónica.

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.

Especialista en Sistemas de Información

- Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
- 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.

Especialista en Administración de Base de Datos

- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicaciones y sistemas.
- 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:

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 del hospital.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos del hospital, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

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.

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.

Especialista en Sistemas de Información

- Realizar la evaluación de las condiciones de las aplicaciones informáticas y sistemas de información durante la emergencia.
- Solicitar los "logs" de las aplicaciones informáticas afectadas durante la emergencia.

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.

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.

Especialista en Seguridad de la Información

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

d. Equipo de Restauración de TIC

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.

Especialista en Redes y Comunicaciones

- Es el responsable del equipo de Restauración de TIC
- Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos del hospital.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI 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.

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 equipos móviles y la central telefónica ubicada en el Centro de Datos.

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.
- Coordinar y monitorear la restauración de aplicaciones y ejecución de pruebas para verificación de funcionalidad.

Especialista en Sistemas de Información

- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones del hospital.

- En caso se quiera desplegar y/o reinstalar las aplicaciones informáticas y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de las aplicaciones informáticas y sistemas de información del hospital.

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.

Técnico de Soporte

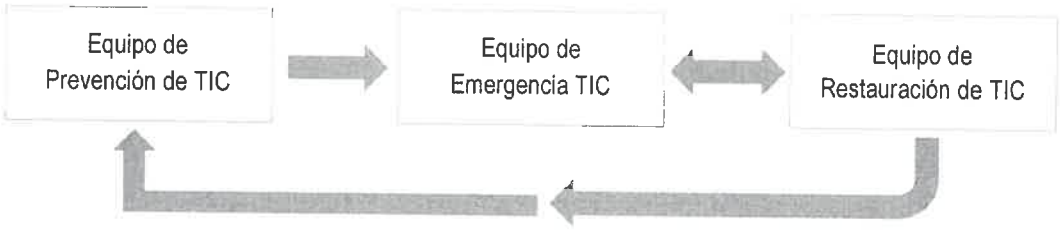
- Verificar el funcionamiento de los equipos personales en las áreas asistenciales y administrativas del hospital, distribuyendo el trabajo entre los técnicos de soporte.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un 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.

Especialista en Seguridad de la Información

- Supervisar la restauración de los servicios de TI.
- 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° 2: Flujo del orden de operación de los equipos de TI



6.2.2 FASE 2: DETERMINACIÓN DE VULNERABILIDADES Y ESCENARIOS DE CONTINGENCIA

En esta fase se procederá a la identificación de las aplicaciones críticas, los recursos 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.

6.2.2.1 Procesos y recursos críticos

A continuación, se detallan los procesos, aplicaciones y recursos críticos, con su respectiva expectativa máxima del tiempo de recuperación:

Tabla N° 1: Procesos y recursos críticos de TI

Proceso Crítico	Aplicaciones y/o Recursos Críticos	Tiempo de Recuperación Objetivo (RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	12 hrs.
	Equipos de protección eléctrica del centro de datos (UPS)	24 hrs.
	Sistema de aire acondicionado del Centro de Datos y Cuartos de Comunicación	24 hrs.
	Infraestructura del Centro de Datos	24 hrs.
	Sistema de Cableado Estructurado	24 hrs.
	Enlaces de cobre y fibra óptica para interconexión con el Centro de Datos	4 hrs.
	Sistema de Almacenamiento de la Información (storage)	24 hrs.
	Medios de respaldo (cintas de backup)	24 hrs.
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	96 hrs.
	Servidores de red en general	98 hrs.
	Sistema de Central Telefónica IP	24 hrs.

Proceso Crítico	Aplicaciones y/o Recursos Críticos	Tiempo de Recuperación Objetivo (RTO)
Gestión de sistemas de información y bases de datos	Sistema de Conectividad y Seguridad Informática	6 hrs.
	Sistemas de información administrativos y portal web	48 hrs.
	Sistemas de información asistenciales	24 hrs.
	Sistema de alarma contra incendios	6 hrs.
	Sistema de Videovigilancia	6 hrs.
	Sistema RIS/PAC	6 hrs.
	Sistema de Llamada de Enfermeras	6 hrs.
	Sistema de Control de Energía (BMS)	6 hrs.
	Sistema de Red Inalámbrica	6 hrs.
	Base de datos y repositorios utilizados por los sistemas y aplicaciones.	48 hrs.
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles, entre otros)	48 hrs.
Operación y mantenimiento de TICs	Sistema de Comunicación VHF/HF	6 hrs.
	Sistema de Sonido Ambiental y Perifoneo	6 hrs.
	Personal crítico responsable de los procesos de TIC.	4 hrs.

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.

6.2.2.2 Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC del hospital, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como la percepción del juicio experto.

Tabla N° 2: Amenazas a los servicios de TI

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.	
06	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 comunicación.	
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
09	Pandemia y/o Epidemia	Ambiental

Determinadas las amenazas que pueden afectar los recursos críticos de TI, 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° 3: Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad estimada
01	Terremoto.	2	4	Moderado
02	Inundación y aniego en el Centro de Datos.	2	2	Menor
03	Falla en telecomunicaciones.	3	4	Moderado
04	Delitos informáticos.	2	4	Moderado
05	Falla del hardware y software.	3	3	Moderado
06	Incendio en el Centro de Datos.	1	3	Menor
07	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicación.	3	3	Moderado
08	Ausencia o no disponibilidad del personal crítico de TI.	2	3	Menor
09	Pandemia y/o Epidemia	2	3	Menor

6.2.2.3 Identificación de Controles Existentes

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

- Cámaras de vigilancia en el interior y exterior del Centro de Datos.
- Grupo electrógeno para el centro de datos.
- 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 comunicación. El mantenimiento está a cargo de la Unidad de Servicios Generales y Mantenimiento.
- Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet.
- Sistema contra incendios en el Centro de Datos.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus 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.

- Garantía vigente de los sub sistemas del sistema de comunicaciones.

6.2.2.4 Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico del hospital, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el punto 6.2.2.2 y de acuerdo a la aplicación de la metodología de riesgos descrita en el Anexo 1, se obtuvo el siguiente resultado:

Tabla N° 4 – Resultado de la evaluación de riesgos de los servicios de TI

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

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

6.2.2.5 Escenarios de riesgo

- Destrucción e indisponibilidad del centro de datos por terremoto o incendio.
- Falla en el funcionamiento de los sistemas de información y portal web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los cuartos de comunicación.

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

Tabla N° 5: Escenarios de Riesgos

Item	Escenario de Riesgo	Descripción	Impacto
01	Destrucción e indisponibilidad del centro de datos por terremoto o incendio	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos	Extremo

Item	Escenario de Riesgo	Descripción	Impacto
		informáticos alojados en el centro datos, como también los componentes del mismo.	
02	Falla en el funcionamiento de los sistemas de información y portal web por delito informático	Se refiere a la falla lógica o caída de los sistemas de información, aplicaciones y portal web, lo cual produce que la información o servicios brindados por ellos no estén disponibles por ataques informáticos.	Extremo
03	Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
04	Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los cuartos de comunicación	Este escenario consiste en el corte o interrupción de las comunicaciones con el centro de datos, así como los servicios publicados en internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionaría caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Alto

6.2.3 FASE 3: ESTRATEGIAS DEL PLAN DE CONTINGENCIA

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

6.2.3.1 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 de TI, 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 de TI. 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 TICs.
- 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 TICs, a cargo del Área de Informática en el Centro de Datos.
- Activación del desvío de las llamadas telefónicas a los usuarios asignados encargados de la atención de la central telefónica.

6.2.3.2 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 de una contingencia:

Acciones durante la contingencia:

- Estudiar y 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.

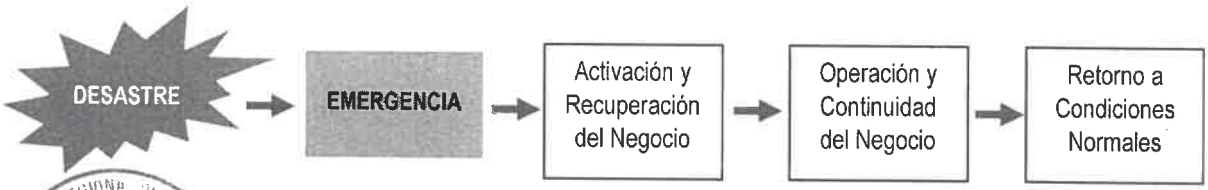
- Informar al responsable del Grupo de Trabajo de Gestión del Riesgo de Desastres sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y 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.

6.2.3.3 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° 3: Ciclo de la estrategia de recuperación de TI



La priorización de la restauración de los servicios de tecnologías de información del hospital se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

Tabla N° 6: Prioridad de atención durante la restauración de TIC

Prioridad de Atención	Descripción
1	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: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGA), Sistemas de Gestión Hospitalaria – SISGALENPLUS, Portal Web institucional, servidores de bases de datos, entre otros.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo equipos de apoyo. Ejemplo: Intranet, entre otros.

En el Anexo 2 y Anexo 3 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.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

6.2.4 FASE 4: ELABORACIÓN DEL PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TIC

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 y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 7: Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Terremoto /Sismo	Extremo	FPC - 01
2	Delito informático (ataque)	Extremo	FPC - 02
3	Falla de hardware y software	Extremo	FPC - 03
4	Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicación.	Alto	FPC - 04

En el Anexo 4 se presenta el desarrollo de cada formato.

6.2.5 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 semestralmente, en los meses de junio 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 en el Anexo N° 05.

6.2.6 FASE 6: IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA

La implementación del presente plan se realizará a partir del segundo mes de su aprobación.

Para tal efecto, el Responsable 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 (TI).
- Participar en las pruebas y simulacros de desastres.

6.2.7 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 de TI.
- Revisión continua de las aplicaciones, 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

VII. CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD PREVENTIVAS	MES 2021			
	SET	OCT	NOV	DIC
Implementación del Plan de Contingencia Informática			X	
Realizar el inventario hardware y software utilizado en el Centro de Datos y Cuartos de Comunicación	X		X	
Ejecutar copias de respaldo (backup)	X	X	X	X
Mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos		X		
Mantenimiento preventivo de los computadores personales, laptops, equipos de impresión, UPS	X	X	X	X

ACTIVIDAD PREVENTIVAS	MES 2021			
	SET	OCT	NOV	DIC
Revisión de obsolescencia tecnológica en los equipos de comunicaciones y de los equipos componentes del Centro de Datos		X		
Revisión de obsolescencia tecnológica en los computadores personales, laptops, equipos de impresión, UPS	X	X	X	X
Actualizar la lista de anexos y teléfonos	X	X	X	X
Actualizar licencia de solución antivirus		X		
Actualizar licencia de equipo de seguridad perimetral				X

VIII. COSTO DEL PLAN

Las actividades del presente plan serán financiadas con las siguientes metas:

- Meta 86 RO (Recursos Ordinarios)

IX. ANEXOS

ANEXO 01

METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. Cálculo de la Probabilidad de Ocurrencia de la Amenaza.

Para realizar este cálculo, se toman en cuenta dos variables: "Ocurrencia" y "Percepción".

Se considera "ocurrencia" a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado al MINAM directamente. Se consideró la siguiente tabla de valores para el cálculo:

N°	Ocurrencia	Descripción
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy Frecuente	Se presentó más de una vez al mes en el último año

La "Percepción" está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

#	Percepción	Descripción
1	Muy Difícil	• <= 1% probabilidad, o • El acontecimiento requiere de circunstancias excepcionales, o • La probabilidad es nula, incluso en un futuro a largo plazo.
2	Difícil	• >1% ó <=10% de probabilidad, o • Puede ocurrir pero no será anticipada
3	Mediana	• >10% ó <=50% de probabilidad, o • Puede ocurrir en el mediano plazo.
4	Posible	• >50% ó <=75% de probabilidad, o • Podría ocurrir anualmente.
5	Muy Posible	• >75% ó 100% de probabilidad, o • El impacto está ocurriendo ahora, o • Podría ocurrir dentro de unos meses.

Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. Identificación de las amenazas que se tomarán en cuenta para la evaluación.

De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

Nivel de Probabilidad Estimada	
Extrema	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja)
Menor	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. Cálculo de la Probabilidad de Afectación del Recurso.

Se utiliza la siguiente tabla de valores para el cálculo:

#	Probabilidad	Descripción
1	Improbable	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados.
2	Baja	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas.
3	Moderada	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
4	Alta	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con el mismo.
5	Muy Alta	Bajo nivel de controles o los controles existentes no son efectivos o eficientes.

4. Cálculo del Impacto del Recurso.

Se utiliza la siguiente tabla de valores para el cálculo:

#	Impacto	Descripción
1	No significativo	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada.
2	Menor	Afecta hasta en 6 horas las operaciones de la sede evaluada.
3	Moderado	Afecta hasta en 24 horas las operaciones de la sede evaluada.
4	Mayor	Afecta hasta en 48 horas las operaciones de la sede evaluada.
5	Catastrófico	Afecta por más de una semana las operaciones de la sede evaluada.

5. Cálculo del Nivel de Riesgo.

Se calcula considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Afectación		Impacto				
		No Significativo (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Muy Alta	(5)	Alto	Alto	Extremo	Extremo	Extremo
Alta	(4)	Moderado	Alto	Alto	Extremo	Extremo
Moderada	(3)	Bajo	Moderado	Alto	Extremo	Extremo
Baja	(2)	Bajo	Bajo	Moderado	Alto	Extremo
Improbable	(1)	Bajo	Bajo	Moderado	Alto	Alto

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Nivel de Riesgo	Interpretación
Extremo	Riesgo no deseable, se requiere acción correctiva inmediata.
Alto	Riesgo no deseable que requiere de una acción correctiva, pero se permite alguna discreción de la gerencia sobre los plazos y compromisos.
Moderado	Riesgo aceptable con revisión de la dirección
Bajo	Riesgo aceptable sin revisión.

ANEXO 02

LISTADO DE APLICACIONES 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	Desktop	1
2	SIAF	Sistema de Información de Administración Financiera	Personal, Presupuesto, Logística, Economía	Desktop	1
3	SIGA	Sistema Informático de Gestión Administrativa	Asistenciales y administrativas	Desktop	1
4	SISMED	Sistema de Gestión de Medicamentos e Insumos	Farmacia	Desktop	1
5	RIS/PAC	Registro y administración de los estudios en el Servicio de Diagnóstico por Imágenes	Diagnóstico por Imágenes y asistenciales	Desktop	1
6	HELPNEX	Sistema de Llamada de Enfermeras	Emergencia, Hospitalización, Centro Quirúrgico	Desktop	1
7	Portal Web Institucional		Asistenciales, administrativas y público en general	Web	2
8	AVIGILON	Sistema de gestión de video vigilancia.	Empresa externa contratada para su operación	Desktop	2
9	BMATIC	Sistema de gestión de colas	Consulta Externa, Emergencia, Diagnóstico por Imágenes, Farmacia, Seguros	Web	2
10	BIOSTAR	Sistema de Control de Asistencia	Asistenciales y administrativas	Desktop	2
11	Sistema de Control de Asistencia	Sistema complementario para la gestión de la información de BIOSTAR y programación de turnos	Asistenciales y administrativas	Desktop	2
12	SIAT	Aplicación para el registro de información para apoyo al tratamiento y el diagnóstico.	Laboratorio, Diagnóstico por Imágenes, Anatomía Patológica	Desktop	2
13	Sistema de Control de Energía - BMS	Permite monitorear el funcionamiento de los equipo eléctricos y electromecánicos	Mantenimiento	Desktop	3

N°	Sistema / Aplicación	Breve descripción	Área Usuaria	Tipo	Prioridad
13	Sistema de Convocatorias CAS	Permite el registro de la postulación en línea de las convocatorias CAS	Personal	Web	3
14	SFS - Sistema Facturador de la SUNAT	Envío de Información de Comprobantes Electrónicos a la SUNAT	Economía	Web	3
15	SIEOC	Aplicación para el registro de Exámenes Ocupacionales	Consulta Externa	Desktop	3
16	SIEMEL	Aplicación que genera información para la Facturación Electrónica a ser utilizada por el Facturador de la SUNAT	Economía	Desktop	3

ANEXO N° 03

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y CUARTOS DE COMUNICACIÓN 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	1
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de Control de Acceso	2
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de llamada de Enfermeras	1
1	Servidor (virtual)	Aplicaciones	Servidor del Sistema de Gestión de Colas	2
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 de Gestión Hospitalaria (SISGALEN PRUEBAS)	1
1	Servidor (virtual)	Aplicaciones	Servidor para Sistema Integrado de Gestion Administrativa (SIGA)	1
1	Servidor (virtual)	Aplicaciones	Servidor para el Sistema de Integrado de Administración Financiera (SIAF)	1
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

CENTRO DE DATOS				
Cant.	Tipo de Equipo	Rol	Descripción	Prioridad
1	Equipo Firewall	Seguridad	Equipo FORTINET para gestionar políticas de seguridad	1
1	Equipo	Controlador de red	Equipo para el Sistema de Red Inalámbrica	2
1	Equipo	Reloj Patrón	Sistema de Relojes Sincornizados 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
		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

CUARTO DE COMUNICACIONES					
N °	Ambiente	Tipo Equipo	Cant.	Descripción	Prioridad
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 04:

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

HRM	Evento: Terremoto/ Sismo	FPC – 01

1.PLAN DE PREVENCIÓN

a. **Descripción del evento**

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- Oficinas y/o Centro de Datos Principal.

Información

- Personal de la entidad.

b. **Objetivo**

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del Hospital, sin exponer la seguridad de las personas.

c. **Entorno**

Este evento puede afectar las instalaciones del Hospital y el Centro de Datos, al ubicarse en la misma ciudad.

d. **Personal Encargado**

El Grupo de Trabajo de Gestión del Riesgo de Desastres del Hospital, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e. **Condiciones de Prevención de Riesgo**

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones del Hospital, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realización de simulacros de evacuación con la participación de todo el personal del Hospital
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f. Acciones del Equipo de Prevención de TIC

- Evaluar en coordinación con el Grupo de Trabajo de Gestión del Riesgo de Desastres el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portal de la entidad.

2.PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos Relacionados antes del evento

- Tener la lista actualizada del personal por Departamentos, Oficinas, Unidades y Áreas.
- Mantenimiento del orden y limpieza del Hospital y el Centro de Datos.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c. Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC.

d. Personal Encargado

Equipo de Emergencia de TIC

e. Descripción de las actividades después de activar la contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros liquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de las Brigadas Hospitalarias, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal del Hospital que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.

HRM	Evento: Terremoto/ Sismo	FPC – 01

- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del Hospital, para las acciones que deban ser efectuadas por ellos.
- En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la jefe/a de la Unidad de Estadística e Informática deberá coordinar con el Director/a del Hospital.

f. **Duración**

Los procesos de evacuación del personal del Hospital deberán ser calmados y demorar 5 minutos como máximo.
La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3.PLAN DE RECUPERACIÓN

a. **Personal Encargado**

El personal encargado es el/la Coordinador/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del Hospital.

b. **Descripción de actividades**

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

En caso, el evento haya sido de considerable magnitud, se deberá:

- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Movilizar los equipos de respaldo al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Trabajo de Gestión del Riesgo de Desastres.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
  - Confirmar los puntos de recuperación de datos de las aplicaciones.
  - Verificar que las funcionalidades de comunicación están funcionando correctamente.
  - Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
  - Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.

HRM	Evento: Terremoto/ Sismo	FPC – 01

- Registrar todos los gastos operacionales relacionados con la continuidad de los servicios del hospital.

c. Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TIC, presentará un informe al Grupo de Trabajo de Gestión del Riesgo de Desastres, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d. Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo de Trabajo de Gestión del Riesgo de Desastres.

e. Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TIC, luego del cual se determinará las acciones a tomar.

HRM	Evento: Delito Informático	FPC – 02

1.PLAN DE PREVENCIÓN

a. Descripción del evento

Alteración de datos del portal web y sistemas de información a través de ataque cibernético (hacking) y/o malware.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Sistemas de información, aplicaciones y portal web del Hospital

b. Objetivo

Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c. Entorno

Este evento se puede dar en cualquiera de los servidores y estaciones ubicadas en el Centro de Datos y en el Hospital.

d. Personal Encargado

El Equipo de Prevención de TIC es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

e. Condiciones de Prevención de Riesgo

- Instalación de parches de seguridad en los equipos.
  Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.

- Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que no lo requieran.
- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al personal del Área de Informática, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas Informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f. Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- Llevar un control de versiones de las fuentes de los sistemas de información y portal web de la entidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- Documentar y validar los manuales de restauración de los sistemas de información en producción.

2.PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b. Procesos Relacionados antes del evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c. Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC y el/la especialista de Seguridad de la Información pueden activar la contingencia.

d. Personal Encargado

Equipo de Emergencia de TIC

e. Descripción de las actividades después de activar la contingencia

- Desconectar o retirar de la red de datos del Hospital, el servidor o la estación infectada o vulnerada.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)

HRM	Evento: Delito Informático	FPC – 02

- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
- Probar el sistema, en caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f. Duración

La duración del evento no deberá ser mayor DOS HORAS en caso se confirme la presencia de un virus en estaciones de trabajo y de CUATRO HORAS en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

3.PLAN DE RECUPERACIÓN

a. Personal Encargado

El equipo de restauración de TIC, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portal web, coordinará con el usuario responsable del mismo y/o Jefe del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b. Descripción de actividades

Se informará a el/la Jefe/a de la Unidad de Estadística e Informática del hospital el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- 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.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red del Hospital.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de información afectado.
- Comunicar el restablecimiento del servicio.

En función a esto, el/la especialista de Seguridad de la Información, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del Hospital.

HRM	Evento: Delito Informático	FPC – 02

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad de la información.

c. **Mecanismos de Comprobación**

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.

El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso, presentará un informe a el/la Jefe/a de la Unidad de Estadística e Informática, explicando que parte del servicio 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 del Hospital, se desactivará el presente Plan.

e. **Proceso de Actualización**

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

HRM	Evento: Falla de hardware y software	FPC – 03

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.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Storage

Software

- Aplicaciones usadas por el Hospital y de servicio al ciudadano

Información

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

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.

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.

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 – 03

- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- 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.

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

Disponibilidad de las copias de respaldo.
Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

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

- 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.

e. Duración

El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3.PLAN DE RECUPERACIÓN

a. Personal Encargado

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

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 afectado por falla de los servidores. 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.

HRM	Evento: Falla de hardware y software	FPC – 03

- 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.

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 Especialista en Redes y Comunicaciones, presentará un informe a el/la Jefe/a de la Unidad de Estadística e Informática, explicando que parte del servicio 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 Especialista en Redes y Comunicaciones, quien identifica 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 Especialista en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

HRM	Evento: Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicación	FPC - 04

1.PLAN DE PREVENCIÓN

a. Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos y/o Cuartos de Comunicación.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS y generador eléctrico
- Aire acondicionado

b. Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c. Entorno

Este evento puede darse en el Centro de Datos y/o Cuartos de Comunicaciones, por tener cada una de ellas los cuartos de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d. Personal Encargado

El/La Jefe de la Unidad de Servicios Generales y Mantenimiento y el/la Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e. Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del Hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
  Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 01 hora como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.

HRM	Evento: Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicación	FPC - 04

- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del Hospital (puertas, contactos magnéticos, etc.)
- Verificación del cableado eléctrico de todas las instalaciones del hospital, una vez por año.
- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

f. Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Revisar periódicamente y de forma conjunta con la Unidad de Servicios Generales y Mantenimiento las instalaciones eléctricas del Centro de Datos y Cuartos de Comunicación.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y las instalaciones de Soporte Informático sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos del Hospital.

2.PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia

Corte de suministro de energía eléctrica en los ambientes del hospital.

b. Procesos Relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones.

c. Personal que autoriza la contingencia

El/La Jefe/a de la Unidad de Servicios Generales y Mantenimiento y/o Coordinador de Continuidad de TIC pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia

- Informar a el/la Jefe/a de la Unidad de Estadística e Informática del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar su proceso de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía en el Centro de Datos sea mayor a

HRM	Evento: Falla del suministro eléctrico en el Centro de Datos y cuartos de comunicación	FPC - 04

dos (02) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

e. **Duración**

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

3.PLAN DE RECUPERACIÓN

a. **Personal Encargado**

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

b. **Descripción de actividades**

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información.

Se debe realizar como mínimo las siguientes actividades:

- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguiente detalle:
  - Equipos de Comunicaciones (router, switches core, switches de acceso)
  - Equipos de almacenamiento (storage).
  - Servidores físicos por orden de prioridad
  - Servidores virtuales por orden de prioridad

- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c. **Mecanismos de Comprobación**

El/La Especialista en Redes y Comunicaciones presentará un informe a el/la Jefe/a de la Unidad de Estadística e Informática, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado 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 se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

e. **Proceso de Actualización**

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

ANEXO 05:

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: / /

RESULTADO DE LA PRUEBA

Resultado: Deficiente: ☐ 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 PARTICIPANTES

Participante	Cargo	Firma