PERÚ | Ministerio de Salud

PCRIS
Programa Creación de Redes Integradas de Salud

PROGRAMA CREACIÓN DE REDES INTEGRADAS DE SALUD - PCRIS

Plan de Contingencia y Recuperación de Servicios de TI

2024

INDICE

PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD - PCRIS - COORDINADOR GENERAL

PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD - PCRIS - COORDINACIÓN ASESORÍA LEGAL

PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD - PCRIS - COORDINADOR ADMINISTRATIVO FINANCIERO (E)

1. INTRODUCCIÓN

El presente documento define el Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en el Programa Creación de Redes Integradas de Salud. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

En el marco de la Resolución Ministerial N° 028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno, se señala que el Plan de Continuidad Operativa comprende, entre otros planes específicos, el Plan de Contingencia y el Plan Recuperación de Servicios de Tecnologías de la Información.

El Equipo de Tecnologías de la Información del Programa Creación de Redes Integradas de Salud (PCRIS) ha desarrollado un Plan de Contingencia y Recuperación de los servicios de Tecnología de la Información con el propósito de fortalecer su infraestructura tecnológica. Este plan detalla los pasos a seguir para prevenir, detectar y responder a eventos disruptivos que puedan afectar la disponibilidad y el desempeño de los servicios de TI. A través de este plan, se busca minimizar el impacto de las interrupciones y asegurar una rápida recuperación de las operaciones.

2. FINALIDAD

Asegurar la continuidad de los servicios de tecnología de la información y comunicaciones del Programa Creación de Redes Integradas de Salud, minimizando el impacto de incidentes en las operaciones de la institución y garantizando la prestación ininterrumpida de los servicios a los usuarios internos y externos. Priorizando la recuperación de los sistemas y datos críticos para mantener la productividad y la eficiencia de la institución.

3. BASE LEGAL

- Resolución de Coordinación General N° 01-2022-PCRIS-CG, que aprueba el Manual de Operaciones del Programa Creación de Redes Integradas de Salud.
- Memorando N° D000006-2023-MINSA-PCRIS/CAF, donde se conforma el Equipo de Tecnologías de la Información del PCRIS, siendo quien lo lidera el Responsable de TI.

- Ley N° 29733, Ley de Protección de Datos Personales, modificada por Decreto Legislativo N°1353.
- Resolución Ministerial N° 028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley N° 29733, Ley de Datos personales.

- Resolución Administrativa N° 019-2017-MTC/33.6, que aprueba la Metodología de Gestión de Riesgos de Seguridad de la Información.
- Norma ISO 22301:2012. Seguridad de la Sociedad – Sistemas de Gestión de la Continuidad del Negocio – Requisitos.
- 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.
- Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

4. METODOLOGÍA PARA LA FORMULACIÓN DEL PLAN DE CONTINGENCIA TECNOLÓGICO

El desarrollo del presente Plan seguirá la siguiente metodología basada en fases:

- **Fase 1:** Organización. Definición del objetivo, alcance, participantes y demás aspectos generales del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información
- **Fase 2:** Análisis de la arquitectura tecnológica. Identificación de los activos informáticos (servicios digitales y componentes de la infraestructura tecnológica) relevantes para la continuidad de los procesos institucionales y, por lo tanto, para la priorización de su recuperación en el escenario de interrupción. Dicha priorización se realiza de acuerdo con
  la siguiente valoración:

Prioridad para la recuperación	Descripción	Tiempo de recuperación
Alta	Impacta en servicios al ciudadano y/o a la mayor parte de las coordinaciones de la entidad.	Hasta 12 horas
Media	Impacta en servicios internos y/o a coordinaciones particulares de la entidad.	Hasta 24 horas
Baja	Impacta en servicios de uso individual por algunos puestos de la entidad.	Hasta 72 horas

- **Fase 3: Análisis de riesgos.** Identificación de los riesgos que podrían impactar en la provisión continua de los servicios priorizados en la fase anterior. Incluye la caracterización considerando la probabilidad y el impacto de acuerdo con la siguiente valoración:

Probabilidad de ocurrencia	
Alta	Impacta en servicios al ciudadano y/o a la mayor parte de las coordinaciones de la entidad.
Media	Impacta en servicios internos y/o a coordinaciones particulares de la entidad.
Baja	Impacta en servicios de uso individual por algunos puestos de la entidad.

Grado de impacto	
Alta	Puede afectar los niveles de operación y servicio de los procesos de la entidad, incumplimiento metas y objetivos establecidos, pérdidas considerables, demandas legales y daño a la imagen de la institución.
Media	Afecta a ciertos procesos cuyo impacto es limitado a coordinaciones particulares de la entidad.
Baja	No causa un efecto considerable en la entidad.

	Impacto		
Probabilidad	**Bajo (1)**	**Medio (2)**	**Alto (3)**
Alta (3)	Riesgo moderado (3)	Riesgo importante (6)	Riesgo importante (9)
Media (2)	Riesgo tolerable (2)	Riesgo moderado (4)	Riesgo importante (6)
Baja (1)	Riesgo tolerable (1)	Riesgo tolerable (2)	Riesgo moderado (3)

- **Fase 4: Definición de las estrategias para la contingencia**. Para cada uno de los riesgos evaluados, se definen los procedimientos necesarios tanto en las etapas de prevención, ejecución y restauración. Se establece, además los lineamientos para la planificación y ejecución de las pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y el entrenamiento a los involucrados.

- **Fase 5: Elaboración del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información.** Consolidación de la información generada en las fases previas en el documento denominado Plan de Contingencia Informático, el cual será aprobado mediante acto resolutivo de la Coordinación General.

- **Fase 6: Implementación del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información.** Ejecución y puesta en marcha de los controles definidos en el Plan de Contingencia Informático. Incluye la ejecución del Plan de pruebas a fin de verificar la efectividad de los controles definidos en la mitigación de los riesgos identificados, así como la efectividad de los procedimientos ante escenarios simulados de contingencia.

- **Fase 7: Planificación y ejecución de las pruebas**. Definición de las actividades para realizar las pruebas periódicas del Plan de Contingencia Informático, a fin de verificar su efectividad simulando los escenarios de contingencia descritos.

- **Fase 8: Seguimiento y evaluación.** Incluye el monitoreo continuo de la implementación del Plan de Contingencia Informático, identificando mejoras que deben ser evaluadas e incluidas en las actualizaciones anuales que se realicen.

5. GENERALIDADES

5.1. Objetivos

5.1.1. Objetivo General

Establecer los principios y procedimientos necesarios para mantener la continuidad de los servicios y procesos esenciales del Programa Creación de Redes Integradas de Salud, asegurando la protección de la información, la infraestructura tecnológica y facilitando una respuesta coordinada y efectiva ante cualquier incidente.

5.1.2. Objetivos Específicos

a) Identificar y analizar los posibles riesgos que puede afectar a las plataformas y aplicaciones consideradas críticas para la operación del Programa Creación de Redes Integradas de Salud.

b) Identificar al personal clave interno y externo requerido para la operación de las actividades críticas.

c) Definir la funcionalidad mínima que se requiere en caso de contingencia.

d) Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

e) Elaborar procedimientos específicos para cada servicio critico ante situaciones de emergencia alineados con el plan de contingencia de los servicios de Tecnologías de la Información.

f) Desarrollar y ejecutar programas de capacitación inicial para todo el personal involucrado en el Plan de Contingencia Informático con la finalidad de que sepan cómo responder ante incidentes y garantizar la continuidad de las operaciones críticas.

g) Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan de Contingencia Informático.

5.2 Alcance

El Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información, tiene como alcance garantizar la continuidad operativa de los servicios de Tecnología de la Información críticos para el funcionamiento de la institución, identificando las estrategias a seguir para la mitigación del impacto y recuperación
de los servicios de TI ante una crisis y/o emergencia que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

5.3 Roles y responsabilidades

5.3.1. Organización

Resolución de Coordinación General N° 01-2022-PCRIS se aprueba el Manual de Operaciones del PCRIS, donde indica que la Coordinación Administrativa y Financiera (CAF) es el órgano encargado de coordinar y supervisar las actividades de tecnologías de la información del Programa, dependiente de la Coordinación General, a razón de dicha Coordinación emite el Memorando N° D006-2023-MINSA-PCRIS/CAF donde conforma el Equipo de Tecnologías de la Información que tiene como funciones conducir, ejecutar, supervisar y agilizar el flujo de información entre las coordinaciones de la Entidad.

Para el funcionamiento del Plan de Contingencia y Recuperación de Servicios de Tecnología de la Información, se ha conformado un equipo operativo, exclusivamente integrado por personal del Equipo de Tecnologías de la Información:

5.3.2. Líder de Recuperación de Servicios de TI

- Representado por el Responsable del Equipo de Tecnologías de la Información del Programa Creación de Redes Integradas de Salud.
- Se encarga de analizar, definir y tomar decisiones ante incidentes disruptivos de los servicios informáticos considerados como críticos para los procesos institucionales.
- Dirige las acciones mientras dura el incidente e informa a instancias superiores el desarrollo y resultado final de la recuperación.
- Informa a la Coordinación General y a quien corresponda los avances, resultados y estrategias adoptadas durante la gestión de la contingencia de TI.

5.3.3. Coordinador de Recuperación de Servicios de TI

- Representado por el Oficial de Seguridad y Confianza Digital del Programa Creación de Redes Integradas de Salud.
- Responsable de brindar soporte a la continuidad operativa y de contingencia de TI.
- Coordina con los miembros de los equipos de recuperación las actividades de recuperación y la gestión documentaria.

5.3.4. Equipos de Recuperación de Servicios de TI

- Representado por los consultores del Equipo de Tecnologías de la Información.
- Los equipos de recuperación de TI se encargan de la respuesta al incidente y la recuperación de los servicios de TI que se han visto afectados por la interrupción del servicio.
- Estos equipos se conforman y operan de acuerdo con las indicaciones del Líder de Recuperación de TI y del Coordinador de Recuperación de TI.
- Los miembros de los equipos de recuperación coordinan directamente con sus proveedores de servicio

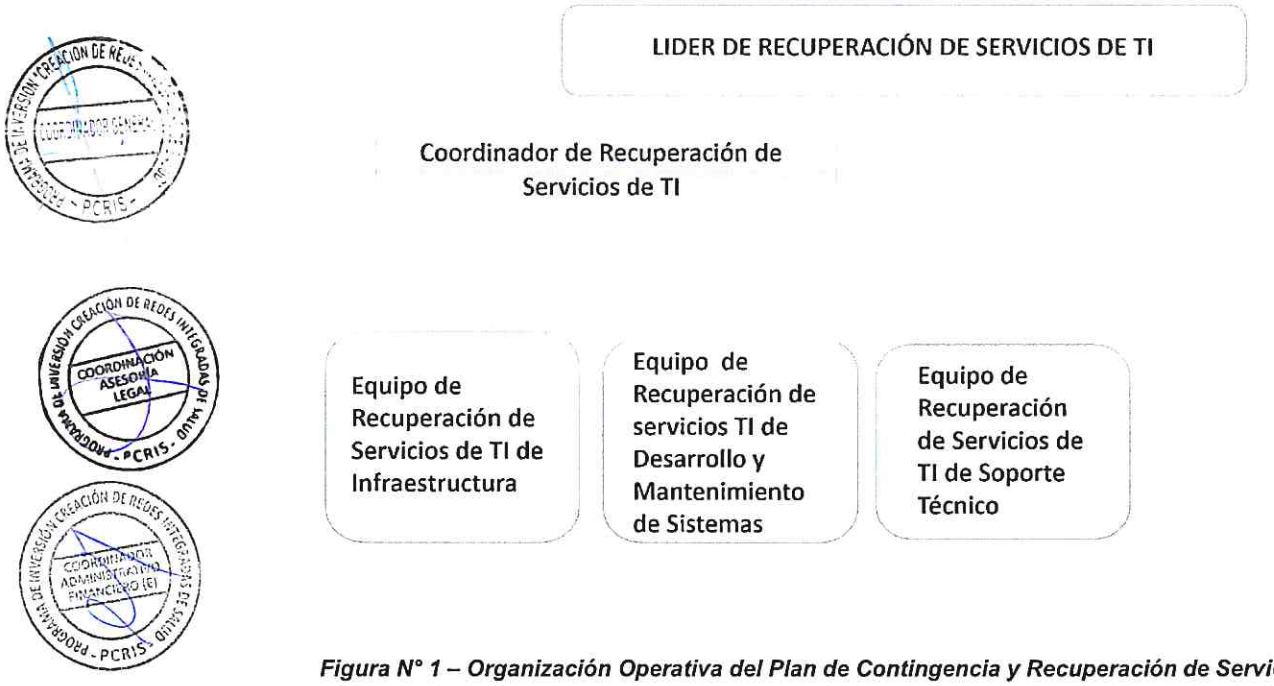


Figura N° 1 – Organización Operativa del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información del PCRIS

De manera adicional:

✓ La Coordinación General es responsable de:

a) Conducir y coordinar, de requerirse, el involucramiento de otras coordinaciones de la organización de la entidad ante la ocurrencia de contingencias, en coordinación con el Equipo de Tecnologías de la Información.

b) Atender los requerimientos del Equipo de Tecnologías de la Información para la planificación de los medios de prevención, así como durante la ejecución y recuperación ante incidentes tecnológicos o desastres.

El Equipo de Tecnologías de la Información es responsable de:

a) Cumplir los procedimientos de respuestas ante cada tipo de los incidentes identificados en el presente Plan.
b) Actualizar el presente Plan.

PROGRAMA DE INVERSIÓN "CREACIÓN DE REDES INTEGRADAS DE SALUD" - PCRIS - COORDINADOR GENERAL

PROGRAMA DE INVERSIÓN "CREACIÓN DE REDES INTEGRADAS DE SALUD" - PCRIS - COORDINACIÓN ASESORÍA LEGAL

PROGRAMA DE INVERSIÓN "CREACIÓN DE REDES INTEGRADAS DE SALUD" - PCRIS - COORDINADOR ADMINISTRATIVO FINANCIERO (E)

5.4 Vinculación con el Plan Estratégico Institucional

El Plan de Contingencia Tecnológico ha sido concebido para establecer procedimientos y acciones de contingencia necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos, que permiten asegurar una pronta y eficaz recuperación de estos.

En ese sentido, el Equipo de Tecnologías de la Información, tiene como propósito proteger la información, asegurando su procesamiento y desarrollo basándose en los objetivos institucionales definidos en el Plan Operativo Institucional (POI), esto es, que coadyuve a la mejora integral de los procesos de soporte administrativo, en el que predomine la automatización, integración, simplicidad y eficacia en su aplicación; y, otro para afrontar la gestión de riesgos en caso de presentarse algún desastre físico.

6. GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **Plan de Contingencia Informático.** Documento de gestión que establece los procedimientos y acciones necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos que soportan los procesos institucionales de la Programa Creación de Redes Integradas de Salud, ante situaciones que pongan en riesgo su funcionamiento.
- **Incidente (de continuidad).** 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 del PCRIS.
- **Riesgo.** Evento que podría interrumpir la provisión de un servicio de TI a los usuarios, impactando en la ejecución de las actividades y/o procesos de las unidades de organización involucradas.
- **Amenaza:** Es cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.
- **Método de análisis de riesgos**: Es el conjunto de técnicas empleadas para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención ante riesgos potenciales y mitigar su impacto.
- **Acciones de prevención.** Actividades, también llamados controles, que tienen la finalidad de evitar o mitigar la materialización de los riesgos identificados en incidentes.
- **Acciones de ejecución.** Actividades que tienen la finalidad de reanudar la provisión de los servicios de TI interrumpidos.

- **Acciones de recuperación.** Actividades que tienen la finalidad de desactivar, una vez superado el incidente de continuidad, las acciones (provisionales) de ejecución que se hayan implementado y retornar a la normalidad los servicios de TI.
- **Plan de Pruebas.** Secuencia de actividades que permiten verificar la efectividad de las acciones de prevención, ejecución y recuperación establecidas en el Plan de Contingencia Informático
- **RTO (Recovery Time Objective):** Se refiere al período de tiempo máximo permitido para la recuperación de los servicios, sistemas o procesos críticos de una organización después de un incidente o interrupción

7. ANÁLISIS DE LA ARQUITECTURA TECNOLÓGICA

7.1 Servicios digitales

En la siguiente tabla se presentan los servicios digitales implementados en el Programa Creación de Redes Integradas de Salud. Actualmente se encuentran 08 sistemas de información en producción. Para ellos, se estima la prioridad para su recuperación y el tiempo objetivo asociado.

N°	Servicio digital (sistema de información y otros)	Tipo	Prioridad para la recuperación	Tiempo de recuperación objetivo (RTO)
1	Mesa de Partes Virtual	Orientado al ciudadano	Alta	Hasta 12 horas
2	Sistema de Gestión Documental (SGD)	Gestión interna	Alta	Hasta 12 horas
3	Sistema Integrado de Gestión Administración (SIGA)	Gestión interna	Media	Hasta 12 horas
4	Sistema Integrado de Administración Financiera (SIAF)	Gestión interna	Alta	Hasta 12 horas
5	Sistema Integrado de Aplicaciones (SIA)	Gestión interna	Media	Hasta 18 horas
6	Software Generador de Reportes Presupuestales (MELISSA)	Gestión interna	Baja	Hasta 24 horas
7	Sistema Modulo de Ejecución de Proyecto para BID y Banco Mundial (SYSMEP)	Gestión interna	Baja	Hasta 24 horas
8	Repositorios para almacenamiento de información	Gestión interna	Media	Hasta 18 horas

7.2 Infraestructura tecnológica

En la siguiente tabla se presentan los componentes de la plataforma tecnológica (incluyendo los servicios base) implementada en el Programa Creación de Redes Integradas de Salud. Para ellos, se estima la prioridad para su recuperación y el tiempo objetivo asociado.

N°	Equipamiento y/o servicio	Tipo	Prioridad para la recuperación	Tiempo de recuperación objetivo (RTO)
1	Servicio de internet de alta velocidad	Gestión interna	Alta	Hasta 12 horas
2	Servicio de seguridad perimetral	Gestión interna	Alta	Hasta 12 horas
3	Sistema de almacenamiento NAS	Gestión interna	Alta	Hasta 6 horas
4	Servidor de BD Producción SQL	Gestión interna	Alta	Hasta 6 horas
5	Equipo servidores de producción (mesa de partes virtual)	Orientado al ciudadano	Alta	Hasta 6 horas
6	Servidor de correo electrónico – Office 365	Orientado al ciudadano / Gestión interna	Alta	Hasta 6 horas
7	Servidor de Gestión de contenidos - SharePoint	Gestión interna	Alta	Hasta 4 horas

8. ANÁLISIS DE RIESGOS

Los sistemas y servicios informáticos están expuestos a riesgos de diferente tipo y naturaleza que pueden afectar su normal funcionamiento, razón por la cual los problemas potenciales se han clasificado en grupos de acuerdo con los factores que determinan su origen, los cuales se describen a continuación:

8.1 Factores de recursos humanos

Están relacionados con la ausencia o presencia insuficiente del personal que trabaja en el mantenimiento y operación de las aplicaciones informáticas. Podrían causar demoras en la atención de desperfectos, daños a los archivos, equipos y otros dispositivos que requieren personal entrenado y calificado para su operación.

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 1.1	Ausencia o presencia insuficiente de personal del Equipo de Tecnologías de la Información	Media	Alto	Riesgo moderado	El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.

8.2 Factores de sistemas

Estos riegos están asociados con el funcionamiento de los equipos, cuyo deterioro o mal uso puede implicar lo siguiente:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 2.1	Falla en los dispositivos de comunicaciones	Media	Alto	Riesgo importante	Paralización total de las comunicaciones de toda la red del PCRIS o un segmento de esta.
Riesgo 2.2	Fallas en las computadoras de escritorio y computadoras portátiles	Media	Alto	Riesgo importante	Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.
Riesgo 2.3	Fallas en los servidores	Media	Alto	Riesgo importante	Paralización en la atención de Usuarios internos que utilicen las aplicaciones de los servidores afectados.

Riesgo 2.4	Daños o perdida de la información en las bases de datos	Media	Alto	Riesgo importante	La pérdida total o parcial de la información ocasionarla problemas en la atención en línea y en la emisión de resultados.
Riesgo 2.5	Acceso de personas no autorizadas a los sistemas informáticos del PCRIS de manera remota	Media	Alto	Riesgo importante	Alteración o pérdida de información de los sistemas de información Difusión de información confidencial Ataque de denegación de servicio que, sin vulnerar la confidencialidad de la información interna
Riesgo 2.6	Infección de virus informáticos en las computador	Media	Alto	Riesgo importante	Lentitud en el funcionamiento de los equipos informáticos Modificaciones en los archivos o pérdida de información Mensajes de error
Riesgo 2.7	Fallas en la funcionalidad de los sistemas de información	Media	Alto	Riesgo importante	Paralización en la ejecución de los procesos institucionales que utilicen los sistemas de información afectados Errores en los registros de los datos, a través de los sistemas de información

8.3 Factores de servicios

Los riesgos identificados en este grupo pueden generar la interrupción de los sistemas y servicios informáticos, afectando las actividades administrativas y de atención al público. Se considera dentro de este grupo el siguiente factor:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 3.1	Corte de suministro de energía eléctrica	Media	Alto	Riesgo importante	Paralización total de las actividades del PCRIS Servicio restringido, se mantendría la operatividad con equipamiento mínimo
Riesgo 3.2	Interrupción del servicio de Internet, Telefonía y otros provistos por terceros	Media	Alto	Riesgo importante	Paralización total de las actividades del PCRIS

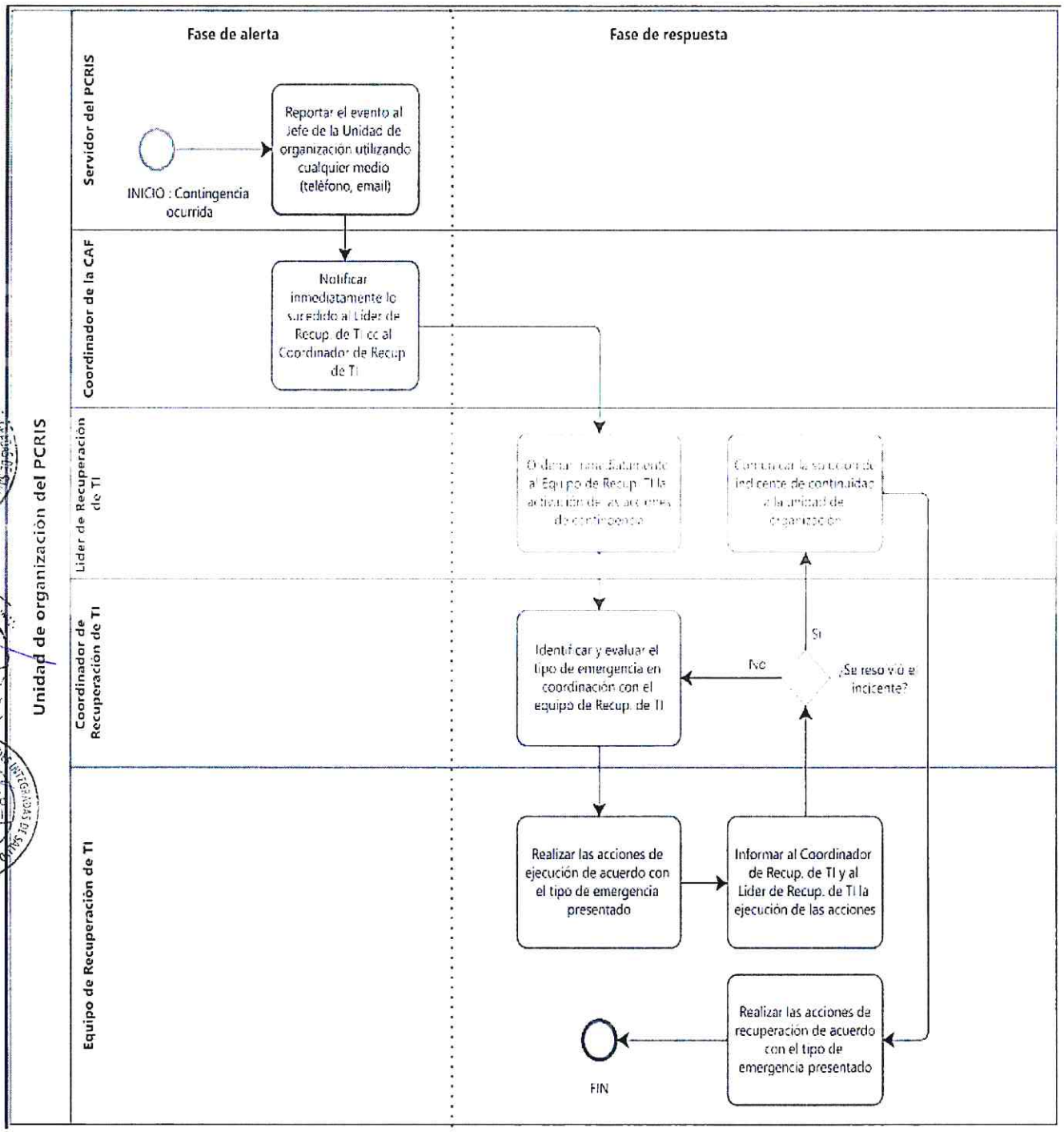
8.4 Factores naturales y artificiales

Son originados por causas externas a la institución y cuyo grado de previsión es muy reducido. Estos percances pueden generar pérdidas o daños físicos en el local del Programa Creación de Redes Integradas de Salud (equipos, mobiliario, inclusive a las personas). Se consideran dentro de este grupo los siguientes:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 4.1	Desastres naturales (terremotos, tsunamis, entre otros)	Baja	Alto	Riesgo moderado	Posible deterioro o inutilización parcial de la infraestructura física del local del PCRIS. En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones). Incapacidad temporal para utilizar servicios de tecnologías de la información.
Riesgo 3.2	Interrupción del servicio de Internet, Telefonía y otros provistos por terceros	Baja	Alto	Riesgo moderado	Posible deterioro o inutilización parcial de la infraestructura física del local de PCRIS. En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones). Incapacidad temporal para utilizar servicios de tecnologías de la información.

9. PROCEDIMIENTOS PARA LA CONTINGENCIA

Las actividades para la atención de los escenarios de contingencia se organizan en dos fases: alerta y respuesta.



9.1 Fase de alerta

a) Se produce el incidente o se materializa una contingencia, llámese emergencia.

b) Es responsabilidad del servidor de la PCRIS que identificó la emergencia, reportar el evento al jefe de la unidad de organización a la que pertenece utilizando cualquier medio de los que encuentre disponibles (teléfono, correo electrónico o en persona).

c) El responsable de la unidad de organización notifica inmediatamente lo sucedido al Líder de Recuperación de TI con copia al Coordinador de Recuperación de TI.

9.2 Fase de respuesta

a) El Líder de Recuperación de TI ordena inmediatamente al Equipo de Recuperación de TI la activación de las acciones de contingencia de acuerdo con los ámbitos pertinentes.

b) El Coordinador de Recuperación de TI identifica y evalúa el tipo de emergencia a atender (ámbito funcional) en coordinación con el Equipo de Recuperación de TI.

c) El Equipo de Recuperación de TI realiza las acciones de ejecución de acuerdo con el tipo de emergencia presentado para restablecer la continuidad de las operaciones. De ser necesario se coordinará con empresas, proveedores de servicios, autoridades locales y nacionales y otras instituciones.

d) El Equipo de Recuperación de TI informa al Coordinador de Recuperación de TI y al Líder de Recuperación de TI la ejecución de las acciones de contingencia.

e) De no resolverse el incidente de continuidad de los servicios de TI, se realizan las actividades a partir del inciso b. de la fase de respuesta.

f) De resolverse el incidente de continuidad de los servicios de TI, el Líder de Recuperación de TI comunica a la unidad de organización afectada la solución de dicho incidente.

g) El jefe de la unidad de organización valida el restablecimiento del servicio TI interrumpido y da la conformidad a la solución implementada.

h) El Equipo de Recuperación de TI realiza las acciones de recuperación de acuerdo con el tipo de emergencia presentado para retornar a la normalidad los servicios de TI. De ser necesario se coordinará con empresas, proveedores de servicios, autoridades locales y nacionales y otras instituciones.

9.3 Procedimientos para la continuidad de servicios

A continuación, se detallan las medidas preventivas, de ejecución y recuperación, que deberán ser aplicados para minimizar los riesgos de interrupción de los sistemas informáticos; de acuerdo con el grado de impacto de los riesgos, así con su probabilidad de ocurrencia y posibles efectos.

9.3.1. Factores de recursos humanos

Riesgo 1.1.	**Ausencia de personal del Equipo de Tecnologías de la Información**		
Probabilidad de ocurrencia	**Media**	**Grado de impacto**	**Alto**
Efecto	Se podría ver afectada la operatividad de los servicios informáticos y la adecuada atención a los usuarios.		
	El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.		
Acciones de prevenciones	Implementar manuales de operaciones y procedimientos en los que se señale las labores que llevan a cabo por cada proceso crítico de los sistemas informáticos.		
	Elaborar una lista de los sistemas informáticos críticos, con el nombre y número de teléfono del encargado de cada sistema y el de su reemplazo en caso de emergencia. Esta lista será actualizada cada vez que cambie el personal del Equipo de Tecnologías de la Información o rote de funciones.		
	Almacenar las credenciales de acceso (usuarios y claves) con permiso de administrador, de los equipos del Centro de Datos en sobres lacrados, los cuales deberán estar bajo la custodia del Responsable del Equipo de Tecnologías de la Información.		
Acciones de ejecución	El personal de reemplazo asume las funciones del personal titular en caso de emergencia.		
	Brindar al personal de reemplazo todos los accesos necesarios para que cumpla con las labores encargadas.		
	Brindar al personal de reemplazo los usuarios y claves con permiso de administrador, de ser necesario.		
Acciones de recuperación	Retirar los accesos brindados al personal de reemplazo una vez recuperados los servicios.		
	Realizar el cambio de las claves y generar nuevos sobres lacrados de credenciales de acceso a los equipos del Centro de Datos, en el caso que los anteriores sobres hayan sido abiertos.		

9.3.2. Factores de sistemas

Riesgo 2.1.	**Fallas en dispositivos de comunicaciones**		
Probabilidad de ocurrencia	**Media**	**Grado de impacto**	**Alto**
Efecto	Paralización total de las comunicaciones de toda la red del Programa Creación de Redes Integradas de Salud o un segmento de esta.		
Acciones de prevención	Realizar el mantenimiento preventivo de los equipos de comunicaciones, de acuerdo con lo establecido por el Equipo de Tecnologías de la Información.		
	Mantener un stock de reposición de controladores de red y dispositivos de comunicaciones que garanticen su reemplazo inmediato en el caso que sufran fallas.		
	Capacitar al personal responsable de los equipos de comunicaciones, del Equipo de Tecnologías de la Información, sobre la configuración de los equipos informáticos.		
	Elaborar, ejecutar y actualizar el Plan de renovación de los equipos de comunicaciones de acuerdo con su vida útil y grado de uso.		
Acciones de ejecución	Verificar las conexiones de los hubs, switches y routers, entre otros equipos de comunicaciones.		
	Reiniciar el equipo de comunicaciones que esté fallando.		
	Verificar la configuración del equipo de comunicaciones que esté fallando.		
	Si no se obtiene un funcionamiento óptimo, cambiar el equipo de comunicaciones por el equipo de comunicaciones de respaldo y proceder a efectuar la configuración necesaria.		
Acciones de recuperación	Verificar las posibles fallas en el equipo de comunicaciones; en el caso de detectarse alguna, coordinar con el proveedor su reparación o adquirir otro equipo de comunicaciones para su reemplazo		
	Poner operativo el equipo de comunicaciones de respaldo.		
	Estabilizar la red de datos de la sede central y restablecer los enlaces con las demás sedes.		

Riesgo 2.2.	**Fallas en las computadoras de escritorio o las computadoras portátiles**		
Probabilidad de ocurrencia	**Media**	**Grado de impacto**	**Alto**
Efecto	Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.		
Acciones de prevención	Realizar el mantenimiento preventivo de las computadoras de escritorio y computadoras portátiles del PCRIS de acuerdo con Plan de Mantenimiento establecido por el Equipo de Tecnologías de la información.		
	Instalar y actualizar software antivirus en todas las computadoras de escritorio y computadoras portátiles del PCRIS.		
	Concientizar a los usuarios sobre las buenas prácticas en el uso de las computadoras de escritorio y computadoras portátiles para minimizar la ocurrencia de posibles fallas en estos equipos, en las capacitaciones realizadas por el Equipo de Tecnologías de la Información.		
	Elaborar, ejecutar y actualizar el plan de renovación de los equipos de oficina de acuerdo con su vida útil y grado de uso.		

Acciones de ejecución	Verificar el origen de la falla y estimar el tiempo que tomará la reparación; si es menor a una hora, efectuar la reparación en el lugar del usuario, de lo contrario se procede a retirar el equipo para su reparación, entregándosele temporalmente al usuario una computadora portátil como equipo de reemplazo hasta que dicho equipo sea reparado y devuelto.
	Analizar las causas de la falla de la computadora de escritorio o computadora portátil para ser reparada y restaurada a su estado operativo, y luego devuelta al usuario asignado. Si no se consigue reparar el equipo, asignar otro con las mismas características al usuario afectado.
Acciones de Recuperación	Restaurar la información del usuario del correo institucional y aquella respaldada por el usuario.

Riesgo 2.3.	**Fallas en los servidores**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Paralización en la atención de usuarios internos que utilicen las aplicaciones de los servidores afectados.		
Acciones de prevención	Realizar el mantenimiento de hardware y software tanto preventivo como correctivo de acuerdo con el Plan de Mantenimiento establecido por el Equipo de Tecnologías de la Información.		
	Verificar que los servidores deben contar con un UPS que asegure su operatividad por un tiempo prolongado ante la falta de suministro de energía eléctrica, de mínimo 1 hora.		
	Realizar un inventario, actualizado anualmente, de todos los programas y archivos de los servidores.		
	Contar con copias de seguridad actualizadas de los servidores.		
	Elaborar, ejecutar y actualizar el Plan de renovación de los servidores de acuerdo con su vida útil y grado de uso.		
Acciones de ejecución	Diagnosticar los inconvenientes presentados en los equipos servidores o virtualizados.		
	Realizar la captura de datos para determinar las fallas presentadas en los servidores físicos o virtualizados.		
Acciones de recuperación	Realizar la restauración desde las copias de seguridad.		
	Realizar la restauración o "snapshot" de los equipos virtualizados.		
	Realizar las pruebas de restauración de datos en los servidores físicos y virtualizados.		

Riesgo 2.4.	**Daños o pérdida de la información en las bases de datos**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	La pérdida total o parcial de la información ocasionaría problemas en la atención en línea y en la emisión de resultados.		
	Paralización temporal a la atención de los usuarios internos y externos del PCRIS.		
Acciones de prevención	Restringir los accesos no autorizados a las bases de datos.		

	Verificar que los registros (logs) incluyan los cambios realizados a las bases de datos con la finalidad de que sean auditables.
	Realizar un inventario anual de las bases de datos y su ubicación en los servidores.
	Actualizar la política de respaldo y restauración de información de las bases de datos.
Acciones de ejecución	Verificar la integridad de los datos realizando una auditoria de la información registrada en los logs.
Acciones de recuperación	Efectuar la restauración de las copias de seguridad de las bases de datos.
	Realizar las pruebas de integridad de la información restaurada y los permisos correspondientes.
	Restaurar los accesos y permisos de acceso de los usuarios.

Riesgo 2.5.	**Acceso de personas no autorizadas a los sistemas informáticos del PCRIS de manera remota o a través de vulnerabilidades**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Alteración o pérdida de información en los sistemas informáticos.		
	Difusión de información confidencial en medios públicos.		
	Ataque de denegación de servicio que, sin vulnerar la confidencialidad de la información interna, hagan inaccesible la página web institucional, el correo electrónico o la navegación por internet por parte del personal.		
Acciones de prevención	Efectuar charlas de capacitación y concientización sobre seguridad de la información para los usuarios, de acuerdo con el Plan de Capacitaciones del Equipo de Tecnologías de la Información.		
	Desactivar de los sistemas informáticos los accesos de los usuarios que dejen de laborar, para evitar que, en su ausencia, otra persona acceda con sus credenciales y pueda manipular la información de los sistemas informáticos.		
	Implementar la política que toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el Responsable del Equipo de Tecnologías de la Información del PCRIS con el debido sustento del encargado del área funcional de desarrollo.		
	Otorgar el acceso a la sala de servidores del PCRIS solo al personal autorizado por el Responsable del Equipo de Tecnologías de la Información.		
	Elaborar una matriz de control de acceso de los usuarios a los diferentes recursos de la red (archivos, base de datos, impresoras, entre otros) especificando las autorizaciones respectivas sobre cada objeto.		
	Limitar el número de intentos para el ingreso correcto de las credenciales de acceso a los sistemas, recursos y servicios informáticos, de acuerdo con la política establecida por el Equipo de Tecnologías de la Información.		
	Forzar a los usuarios a cambiar periódicamente sus contraseñas de acceso, de acuerdo con la política establecida por el Equipo de Tecnologías de la Información.		
Acciones de ejecución	Bloquear el acceso de todos los usuarios al sistema informático inmediatamente sea detectada la intrusión.		
	Cambiar la clave de acceso de los sistemas informáticos afectados.		
	Realizar una copia de seguridad de los sistemas informáticos afectados para realizar un análisis posterior.		
Acciones de recuperación	Realizar un análisis exhaustivo para detectar las vulnerabilidades que pudieron ser utilizadas para la intrusión.		
	Analizar los daños que pudo haber ocasionado la intrusión.		
	De ser necesario, restaurar una copia de seguridad de los sistemas informáticos y subsanar las vulnerabilidades encontradas.		

Riesgo 2.6.	**Infección de virus informáticos en las computadoras**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Lentitud en el funcionamiento de los equipos informáticos.		
	Modificaciones de archivos o pérdida de la información.		
	Mensajes de error.		
Acciones de prevención	Brindar charlas de capacitación y concientización para los usuarios sobre el uso de adecuado del internet y los dispositivos informáticos, de acuerdo con el Plan de Capacitaciones del Equipo de Tecnologías de la Información.		
	Capacitaciones del Equipo de Tecnologías de la Información.		
	Verificar que se cuente con software antivirus instalado, actualizado y activo en todas las computadoras de la entidad.		
Acciones de ejecución	Realizar actividades de mantenimiento preventivo a las computadoras.		
Acciones de recuperación	Realizar un análisis de infección de virus informáticos en las computadoras con un antivirus actualizado y un antimalware.		
	Analizar los daños que pudo haber ocasionado la infección, de ser necesario aplicar el plan de contingencia para "Daños o pérdidas de la información en las bases de datos".		
	Realizar las acciones del plan de recuperación para las "Fallas en las computadoras de escritorio o en las computadoras portátiles".		

Riesgo 2.7.	Fallas en la funcionalidad de los sistemas de información		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Paralización en la ejecución de los procesos institucionales que utilicen los sistemas de información afectados.		
	Errores en los registros de los datos a través de los sistemas de información		
Acciones de prevención	Realizar las actividades de QA/QC (aseguramiento y control de calidad) de software y obteniendo la validación del área usuaria, de manera previa al pase a producción.		
Acciones de ejecución	Realizar un análisis del incidente reportado y definir la acción a tomar: a) caso 1: se conoce el motivo de la falla y la corrección podrá ser realizada en un plazo no mayor a 5 días, b) caso 2: no es posible identificar el motivo de la falla y/o desarrollar la solución se realizará en más de 5 días, en cuyo escenario se desplegará un workaround (solución alternativa) en tanto se defina e implemente una solución definitiva.		
Acciones de recuperación	Identificar las causas de las fallas y realizar las correcciones necesarias a fin de evitar la recurrencia de los incidentes.		

9.3.3. Factores de servicios

Riesgo 3.1.	**Corte de suministro de energía eléctrica**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Paralización total de las actividades del PCRIS. Servicio restringido, se mantendría la operatividad con equipamiento mínimo.		
Acciones de prevención	Efectuar el mantenimiento preventivo de todo el equipamiento informático. Realizar pruebas semestrales a los UPS y adquirir nuevos de ser necesario.		
Acciones de ejecución	Poner en funcionamiento el (los) UPS y/o grupos electrógenos para alimentación de equipos de uso críticos. Comunicarse con el personal responsable de control de suministro de energía eléctrica, para coordinar con el Equipo de Tecnologías de la Información el restablecimiento de ésta. En caso de que la falta de energía eléctrica sea mayor a treinta minutos, se deberán apagar los servidores hasta que el servicio sea restablecido.		
Acciones de recuperación	Verificar si la falta de suministro de energía eléctrica se debe a algún desperfecto ocurrido dentro de la institución, en cuyo caso avisar al personal responsable para que proceda con la reparación del desperfecto; de tratarse de una falta atribuible al proveedor de energía eléctrica, comunicarse con ellos para indicar el problema y solicitar la reposición inmediata del servicio. Esperar a que el suministro de energía eléctrica se restablezca y luego efectuar el encendido de los equipos informáticos del Centro de Datos y del personal.		

Riesgo 3.2.	**Interrupción del servicio de Internet, telefonía y otros provistos por terceros**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	Paralización total de las actividades del Programa Creación de Redes Integradas de Salud.		
Acciones de prevención	Incluir niveles de servicio en los contratos con los proveedores. Evaluar el despliegue de servicios alternativos con proveedores diferentes.		
Acciones de ejecución	Solicitar al proveedor del servicio, la fecha y hora de la restauración del servicio interrumpido (escalar el incidente de ser necesario). Comunicar a las áreas usuarias del servicio interrumpido, la información proporcionada por el proveedor.		
Acciones de recuperación	Solicitar al proveedor un reporte detallando las causas de la interrupción, y la planificación de las medidas correctivas/preventivas que implementará.		

9.3.4. Factores naturales y artificiales

Riesgo 4.1.	**Desastres naturales (terremotos, maremotos, entre otros)**		
Probabilidad de ocurrencia	Baja	**Grado de impacto**	Alto
Efecto	Posible deterioro o inutilización parcial de la infraestructura física del local del PCRIS.		
	En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones).		
	Incapacidad temporal para utilizar servicios de tecnologías de la información.		
Acciones de prevención	Establecer zonas de seguridad en las cuales se proteja al personal, así como los		
	Brindar entrenamiento constante al personal para pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre.		

	Contar con un grupo electrógeno en el PCRIS, que pueda activarse para apoyar a las fuentes de energía alternativa (UPS) en la misión de mantener la operatividad de los sistemas informáticos.
	Contar con mobiliario especial (racks) para los equipos informáticos.
	Fijar los equipos informáticos mediante mecanismos de anclaje a sus respectivas bases, con la finalidad de que ante un movimiento fuerte no sufran caídas.
	Realizar copias de seguridad de los aplicativos y bases de datos más importantes, de acuerdo con la política establecida por el Equipo de Tecnologías de la Información, para asegurar la continuidad de las operaciones.
Acciones de ejecución	Verificar el estado de la infraestructura del Centro de Datos.
	Verificar las conexiones y el adecuado funcionamiento de los equipos de uso crítico.
	De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos de uso crítico, falta de energía eléctrica, falta de servidores o de ocurrir un incendio posterior al desastre natural, se deberá tomar en consideración los pasos establecidos en este plan de contingencia como medida de contención para cada uno de los casos.
Acciones de recuperación	Luego de pasado el desastre natural, evaluar los daños ocasionados a la infraestructura tecnológica y física del centro de datos y a los equipos informáticos asignados al personal del PCRIS.
	Realizar un inventario general de los sistemas informáticos afectados, indicando el estado de operatividad de los mismos.
	Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración.
	Realizar tareas de recuperación de acuerdo con lo establecido por el Equipo de Tecnologías de la Información

Riesgo 4.2.	**Desastres artificiales**		
Probabilidad de ocurrencia	Baja	**Grado de impacto**	Alto
Efecto	Posible deterioro de los equipos informáticos del PCRIS.		
	En casos muy graves, la inutilización total de los equipos de uso crítico.		
	Incapacidad temporal para utilizar los servicios de tecnologías de la información.		
Acciones de prevención	Implementar sistemas de detección y extinción de fuego (alarmas de humo y extinguidores de gas) en el Centro de Datos.		
	Implementar sistema de video vigilancia en el Centro de Datos, para vigilancia y monitoreo de los ingresos y así evitar sabotajes por ingresos no autorizados que ocasionen un desastre mayor.		
	Efectuar revisiones anuales del estado de conservación del cableado de energía eléctrica.		
	Contar con personal o servicio de vigilancia las 24 horas del día, con el fin de garantizar la seguridad de la sede del PCRIS de los equipos informáticos que procesan y almacenan toda la información de la institución.		
	Realizar anualmente entrenamiento del personal del Equipo de Tecnologías de la Información para que pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre.		
	Brindar mantenimiento y recarga a los extintores de incendios.		

Acciones de ejecución	Si el fuego es controlable, intentar apagado haciendo uso de los extintores apropiados para cada tipo de incendio.
	Retirar todos los objetos inflamables que se encuentren cerca del fuego.
	De ser posible, desconectar y retirar los equipos informáticos a un ambiente libre de fuego.
	De no extinguirse el fuego, evaluar las instalaciones.
	De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos informáticos, falta de energía eléctrica o falla de servidores, tomar en consideración los pasos establecidos en este Plan de contingencia, como medida de contención para cada uno de los casos.
Acciones de recuperación	Luego de extinguido el incendio, evaluar los daños ocasionados a los sistemas y equipos informáticos.
	Realizar un inventario general de los sistemas y equipos informáticos afectados, indicando el estado de operatividad de los mismos.
	Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración.
	Efectuar tareas de recuperación, de acuerdo con lo establecido por el Equipo de Tecnologías de la Información.

10. PLAN DE PRUEBAS

Los procedimientos para la contingencia definidos en el presente Plan deben ejecutarse en un ambiente de pruebas que simule los eventos de contingencia establecidos; con la finalidad de verificar su efectividad. Dichas pruebas deben realizarse de manera semestral y será planificada, organizada y realizada por el Equipo de Tecnologías de la Información. La información recolectada debe registrarse en el formato 01 anexo 1.

11. ENTRENAMIENTO

El personal involucrado en las actividades definidas en el presente plan debe ser capacitados de manera anual en los lineamientos y contenido específico del mismo incluyendo: mecanismos de coordinación y comunicación entre equipos, roles y responsabilidades, y procedimientos para la contingencia de acuerdo con los escenarios establecidos; a fin de asegurar las competencias requeridas para su ejecución.

Dicha capacitación será planificada, organizada y realizada por el Equipo de Tecnologías de la Información.

12. SEGUIMIENTO Y EVALUACIÓN

Una vez culminadas las pruebas de restauración de acuerdo al Plan de Contingencia se debe realizar una evaluación de los resultados, como es tiempo de respuesta y afectación del incidente en la operatividad del PCRIS entre otros.

13. RECURSOS

13.1 Personal

Conforme lo dispone el numeral 5.3. del presente Plan, para la recuperación y/o mantenimiento de la operatividad de los servicios y aplicaciones en el Programa Creación de Redes Integradas de Salud, el Equipo de Tecnologías de la Información debe contar con el equipo operativo calificado, conforme se especifica a continuación:

a) El Responsable del Equipo de Tecnologías de la Información quien lo preside.
b) Oficial de Seguridad Digital y Confianza Digital del PCRIS.
c) Equipo de Recuperación de TI
   - Consultor en Administración de Redes, Servidores y Seguridad Informática.
   - Consultor en sistemas de información y base de datos.
   - Consultor de soporte técnico informático.

13.2 Presupuesto

Las actividades descritas en el presente Plan se financian con el presupuesto institucional asignado a el Equipo de Tecnologías de la Información de la Coordinación Administrativa Financiera del PCRIS.

14. MONITOREO Y MEJORA CONTINUA

Es probable que, durante la evaluación y el control del Plan de Contingencia y Recuperación de los Servicios de Tecnologías de la Información, se detecte la necesidad de realizar ajustes para adecuar las medidas planificadas a la realidad de la contingencia actual.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

15. ANEXOS

15.1 Anexo 1. Formatos

Formato de control y certificación de las Pruebas del Plan de Contingencia Tecnológico

PRUEBA N°

Escenario de Prueba

Area Responsable

INFORMACION DEL PROCESO

Metodología

Alcance

Condiciones de Ejecución

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio ☐ Satisfactorio con observaciones ☐ Deficiente ☐

Observaciones

ACTUALIZACION DEL PLAN DE CONTINGENCIA

Cambios o actualización en el Plan de Contingencia

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma