 <p>ESE HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:


PLAN DE RECUPERACIÓN ANTE DESASTRES



ESE

HOSPITAL DEL SUR

I T A G Ü Í

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:


1. INFORMACION GENERAL

La E.S.E. Hospital del Sur “Gabriel Jaramillo Piedrahita” es una institución de primer nivel de atención, La ESE cuenta con tres sedes ubicadas estratégicamente en tres comunas de las seis del Municipio de Itagüí con el fin de garantizar una mejor accesibilidad a la población objeto, así:

- *Sede San Pío:* Calle 33 N° 50 A 25
- *Sede Santamaría:* Cra 52 n 78-158
- *Sede Calatrava:* Calle 63 N° 58 FF 11

Las sedes se encuentran interconectadas a través de un canal de fibra óptica.

SERVICIO	CARACTERÍSTICA
Urgencias	Atención de urgencias de Primer Nivel de complejidad en la Sede San Pio los 7 días de la semana 24 horas
Consulta Medica	Disposición de Agendas para consulta externa con médico general en 3 Sedes Santa María, San Pio y Calatrava, horarios de lunes a viernes 07:00 am hasta las 18:00 pm
Hospitalización	Disposición de 9 camas habilitadas para hospitalización de primer nivel; 4 camas de trabajo de parto y postparto y una sala dotada para la atención del parto de baja complejidad. En la Sede San Pio los 7 días de la semana 24 horas al día.
Odontología	Se cuenta con odontólogos generales y unidades odontológicas para la atención del usuario programado en las Sedes Santamaría y Calatrava, además en la sede San Pio con odontología estética.
Programas de PyP	Cuenta con el ofrecimiento de todos los programas de PyP en las Sedes Santa María, San pio y Calatrava para la atención según Resolución 412 de 2000 en horario de 07:00am a 18:00pm.
Servicios de apoyo	<ul style="list-style-type: none"> – Laboratorio: Se cuenta con servicios de Laboratorio Clínico de Primer nivel las 24 horas disponible para el servicio de urgencias y hospitalización según necesidad médica; y para la atención ambulatoria de lunes a viernes de 6 am a 6 pm – Farmacia: El servicio farmacéutico presta su servicio en la sede Santa María y San Pio entregando medicación del POS según prescripción – Imaginología: Se prestan servicios de imágenes diagnósticas para Urgencias, Hospitalización y Consulta externa, en la sede san Pio.

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

	– Procedimientos: Se realizan procedimientos según necesidad para el apoyo en el diagnóstico y tratamiento médico
Procesos Administrativos	–

1.1 OBJETIVO GENERAL

Definir el conjunto de actividades, roles y responsabilidades que permitan mantener la continuidad de la plataforma tecnológica de la ESE, en caso de la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente.

1.2 RESPONSABLE


- ✓ Gerente
- ✓ Subgerencia Administrativa y Financiera
- ✓ Profesional Universitario Ingeniero de Sistemas
- ✓ Técnicos Operativos de Sistemas

1.3 ALCANCE


Este plan se enmarca en la protección de los sistemas y plataformas tecnológicas de la ESE Hospital del Sur “G.J.P.” relacionadas en el Anexo 1.

1.4 DEFINICIONES

- ✓ **Activos tecnológicos:** Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos desde su Misión. Se pueden agrupar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.
- ✓ **BCP:** Sigla en inglés (**Business Continuity Plan**) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.
- ✓ **BIA:** Sigla en inglés (Business Impact Analysis), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.
- ✓ **CAP:** Centro Alterno de Procesamiento. Hace referencia a las instalaciones físicas donde se procesará información en caso de una contingencia mayor en el centro de datos principal.

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

- ✓ **CAO:** Centro Alterno de Operación. Hace referencia al sitio donde operará la entidad en caso de que exista un evento que impida la operación en las instalaciones normales.
- ✓ **CCP:** Centro de Computo Principal. Hace referencia a las instalaciones físicas donde se procesa normalmente la información y donde se encuentra la infraestructura tecnológica en funcionamiento normal.
- ✓ **DRP:** Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.
- ✓ **ERA:** Sigla en inglés (Environment Risk Analysis), Análisis de Riesgos Ambientales en español, y hace referencia a un documento que relaciona los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.
- ✓ **Evento:** Suceso imprevisto que puede ocurrir en un espacio y tiempo específico, generando impactos sobre los activos tecnológicos y activos del negocio.
- ✓ **Plataforma tecnológica crítica:** Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.
- ✓ **RAS:** Sigla en inglés (Response Alternative and Solutions), y hace referencia a un documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.
- ✓ **RPO:** Sigla en inglés (Recovery Point Objective), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.
- ✓ **RTO:** Sigla en inglés (Recovery Time Objective), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.
- ✓ **Nivel de Criticidad,** Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.


- ✓ **Interrupción**, Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la Entidad.
- ✓ **Registro vital**, Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas.

2. CONDICIONES GENERALES

2.1. El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales y de apoyo de la ESE Hospital del Sur “G.J.P.”

2.2. Condiciones Iniciales:

- ✓ Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- ✓ Los funcionarios que ejecutan el plan, o sus suplentes, se encuentran disponibles y no han sido afectados por el desastre.
- ✓ El desastre no afectó simultáneamente el Centro de datos principal y el Centro de datos Alterno.
- ✓ El Centro de datos Alterno estará habilitado para un promedio de 100 usuarios concurrentes.
- ✓ Solo el funcionario responsable activará el DRP.
- ✓ Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han sido efectivas.
- ✓ Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- ✓ Los Backups de las bases de datos e información se realiza de acuerdo a los procedimientos y cronogramas establecidos.

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

3. GUIA DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

3.1 Posible escenario del Desastre.

Los escenarios de desastre, interrupción mayor o un evento contingente que contempla este documento son:

3.1.1. Centro de Datos.

No disponibilidad del centro de cómputo por:

- ✓ Incendio
- ✓ Inundación
- ✓ Terremoto
- ✓ Daño en suministro eléctrico
- ✓ Daño sistema aire acondicionado

3.1.2. Infraestructura de Comunicaciones:


No disponibilidad de los servicios de comunicaciones por fallas en:

- ✓ Switches principales
- ✓ Fibras ópticas de conexión con centros de datos
- ✓ Router principal
- ✓ Enlaces de comunicación con ISP
- ✓ Enlaces de comunicación con sedes
- ✓ Firewall

3.1.3. Servidores

No disponibilidad de la infraestructura por fallas en:

- ✓ MARTE (Servidor de Dominio Principal)
- ✓ KRYPTON (Servidor de Dominio Alternativo)
- ✓ URANO (Servidor de Base de Datos)
- ✓ PLUTON (Servidor Virtualización)
- ✓ JUPITER (Servidor Virtualización)
- ✓ SVRDATOS (Servidor Aplicaciones)

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

3.1.4 Infraestructura de Bases de datos, Almacenamiento y Respaldo

No disponibilidad de datos e información por:

- ✓ Corrupción de la base de datos
- ✓ Borrado o pérdida de datos
- ✓ Falla total o parcial de la SAN
- ✓ Falla total o parcial Discos duros Almacenamiento Externo.
- ✓ Perdida de Discos duros de almacenamiento Externo.
- ✓ Falla en Control de calidad de Backup.

3.1.5. Infraestructura de Aplicaciones


No disponibilidad de la aplicación por:

- ✓ No conexión con otras aplicaciones
- ✓ Borrado o pérdida de datos
- ✓ Integridad de los datos

3.1.6. Servicios tecnológicos

No disponibilidad de la aplicación por:

- ✓ Bloqueo de puertos
- ✓ Fallas en servidores de aplicaciones
- ✓ Virus informativos
- ✓ Ataques de denegación de Servicios.

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

3.2. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada.



Las responsabilidades definidas para cada rol son:


Rol	Antes del evento	Durante el evento	Después del evento
Líder del DRP	<ul style="list-style-type: none"> - Velar por la actualización del DRP y gestionar los recursos requeridos. - Velar por la actualización, distribución y pruebas del DRP. - Comunicar a las personas que corresponda sobre la situación de contingencia. 	<ul style="list-style-type: none"> - Evaluar y activar el DRP y las estrategias de recuperación y Contingencia. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución - Informar el momento en que opera en contingencia y que 	<ul style="list-style-type: none"> - Realizar plan de Mejoramiento acorde con los inconvenientes y oportunidades de mejora identificados durante el evento de Interrupción. - Informar al personal de apoyo sobre el retorno a la Normalidad.



**PLAN DE RECUPERACIÓN ANTE
DESASTRES – DRP**

Código:
Versión: 1
Fecha Actualización:
Elaborado Por:

		<p>puede suceder con la prestación del Servicio</p> <ul style="list-style-type: none"> - Liderar la operación bajo contingencia. - Comunicar a la dirección el desastre, interrupción o evento contingente. - Comunicar a los proveedores la activación del DRP. - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Liderar el retorno a la normalidad. 	
Técnicos Operativos de Sistemas	<ul style="list-style-type: none"> - Comunicar las necesidades de mejoramiento del DRP. - Participar en la ejecución de las pruebas al DRP. - Coordinar actividades de entrenamiento, documentación y actualización del DRP. - Coordinar las actividades de pruebas del DRP. - Identificar los recursos requeridos para la operación del DRP. 	<ul style="list-style-type: none"> Participar de la evaluación el desastre, interrupción o evento contingente. - Comunicar el evento al Líder del DRP - Ejecutar las guías de contingencia y recuperación. - Comunicar al Personal de apoyo Sobre el estado de la operación de Contingencia. - Participar en el alistamiento y disponibilidad del Centro de datos Alterno. - Participar de la corrección del componente afectado y realizar Seguimiento de la solución. - Dar una correcta información a las Personas que lo requieran. - Mantener informado al Líder del DRP. - Coordinar con los responsables el desplazamiento al Centro de datos alterno. 	<ul style="list-style-type: none"> - Participar en las actividades de evaluación y elaboración de planes de Mejoramiento.


	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

		<ul style="list-style-type: none"> - Verificar ejecución del plan de recuperación de desastres. - Participar en la toma de decisiones que se den pro ajustes durante la ejecución del plan. - Coordinar que todo el personal involucrado este participando. 	
Personal de Apoyo (Gesis - Comunicaciones)	Participar en los procesos de divulgación y pruebas al DRP.	<ul style="list-style-type: none"> - Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia. - Informar a todo el personal sobre sobre la situación del evento. - Coordinar la logística de desplazamiento, si es requerido - Contacto con proveedores, si es Requerido 	- Participar en las actividades de evaluación y elaboración de planes de Mejoramiento.

3.3. ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP.

3.3.1. Responsables del reporte del evento

- a. Los usuarios deben reportar el incidente a la mesa de ayuda, o cualquier otro medio que tengan disponible cuando se presente un incidente, interrupción mayor o un evento contingente, en las siguientes situaciones:
- ✓ NO hay acceso a los sistemas de información.
 - ✓ NO hay red de comunicaciones.
 - ✓ NO hay servicio de correo electrónico.
 - ✓ NO hay disponibilidad del canal del comunicaciones.
 - ✓ CUALQUIER otro evento de tecnología que afecte la prestación del servicio.


 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

- b. **Cualquier personal** (vigilancia, servicios generales, Asistencial o Administrativo) debe reportar el incidente a la Oficina de Sistemas cuando:
- ✓ SUENA la alarma contra incendio del centro de Datos,
 - ✓ HAY inundación en piso del centro de datos,
 - ✓ HAY un conato de incendio en el piso donde se encuentre ubicado el centro de Datos y,
 - ✓ CUALQUIER otro evento que afecte o pueda afectar el centro Datos.
- c. El personal del proceso de **Gerencia de Información** encargado del monitoreo de la plataforma (infraestructura de técnica, infraestructura de comunicaciones, infraestructura de datos) deben reportar y atender el incidente cuando:
- ✓ Se detecte caída de servicios,
 - ✓ Se detecte mal funcionamiento de infraestructura crítica (servidores, Dispositivos de comunicaciones, bases de datos) y
 - ✓ Cuando se disparen alarmas ambientales.
- d. **El personal soporte del área de Sistemas** debe atender el incidente de acuerdo a lo establecido en el Procedimiento soporte Informático y se continúa con la ejecución de este Plan si:
- ✓ El incidente afecta la disponibilidad de los sistemas de Información, a nivel general.
 - ✓ El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
 - ✓ Ningún usuario tiene acceso al correo electrónico.
 - ✓ Ningún usuario puede ingresar a las estaciones de trabajo.
 - ✓ Ataque por virus informático.

3.3.2. Responsable de la evaluación del Impacto del Incidente.

El profesional Universitario Ingeniero de Sistemas en compañía de los **Técnicos operativos de Sistemas**, deben realizar un diagnóstico inicial sobre el incidente presentado, teniendo en cuenta:

- ✓ Naturaleza e impacto del incidente.
- ✓ Estrategias definidas en el DRP aplicables u otras soluciones potenciales.
- ✓ Tiempo estimado de solución del incidente.

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

La comunicación con la dirección debe ser constante, con el objeto de solicitar y disponer de ayuda especializada oportuna para atender el incidente en caso de ser necesario.

3.3.3. Activación de un Centro de Datos Alterno.

- a. **El Profesional Universitario Ingeniero de Sistemas**, define si se activa o no un Centro de datos Alterno y deberá informar a la alta dirección el impacto del evento.
- b. En caso de que se active, Líder del DRP debe comunicar la activación al proveedor Involucrado, teniendo en cuenta:
 - ✓ Fecha y hora de inicio de la activación.
 - ✓ Funcionarios de la entidad que estarían en el proceso de activación.
- c. El grupo de trabajo, deberá coordinar la ejecución de las actividades para recuperar la plataforma en el Centro de datos Alterno, teniendo en cuenta:
 - ✓ Enrutamiento y activación de las comunicaciones hacia el Centro de datos Alterno.
 - ✓ Asegurar la replicación de datos.
 - ✓ Verificar la disponibilidad de información en el Centro de datos Alterno.
 - ✓ Configurar y activar los controladores de dominio y sistemas operativos en servidores.
 - ✓ Configurar bases de datos y aplicaciones.

El grupo de soporte deberá realizar las pruebas requeridas para garantizar el acceso a los sistemas de información desde el nuevo centro de datos.


3.4.4 Actividades paralelas.

- a. **El líder del DRP**, deberá solicitar la activación de las contingencias locales teniendo en cuenta los siguientes aspectos:

Daño en las comunicaciones.

- ✓ Configurar el Switch de contingencia, en caso de falla en los switches principales.
- ✓ Contactar al proveedor de comunicaciones, en caso de falla en el enlace de comunicaciones con las sedes.
- ✓ Fallas en el enlace con ISP.
- ✓ Configurar firewall de contingencia, en caso de falla del equipo principal.

Daño en infraestructura de servidores.

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:


Configurar los servidores de contingencia, en caso de falla de alguno de los siguientes servidores:

- ✓ MARTE (Servidor de Dominio Principal), se debe activar el servidor KRYPTON (Servidor de Dominio Alternativo).
- ✓ URANO (Servidor de Base de Datos), se debe activar el servidor PLUTON (Servidor Virtualización) como contingencia y SVRDATOS (Servidor Aplicaciones) como servidor de aplicaciones alternativo.

En caso de no poder utilizar la contingencia, se debe solicitar la adquisición de nueva tecnología.

Daño en Infraestructura de Bases de datos, Almacenamiento y Respaldo:

- ✓ Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de la base de datos, y borrado o pérdida de datos.
 - ✓ Utilizar discos Externos de almacenamiento como contingencia.
- b. En caso de que la falla afecte un equipo que no cuente con garantía y quede en pérdida total, el responsable del proceso solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.
 - c. El responsable del proceso realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.
 - d. El responsable del proceso coordina la solución con el proveedor contratado.
 - e. El responsable del proceso comunica la solución del incidente a la entidad.
 - f. El responsable del proceso, en conjunto con los profesionales especializados, definen la estrategia de retorno a la normalidad, teniendo en cuenta:
 - ✓ Fecha del retorno a operación normal.
 - ✓ Consideraciones especiales a aplicar en el proceso de retorno.
 - ✓ Consideraciones especiales con respecto a la recuperación de la información y mantener la integridad de los datos, cuando aplique.
 - g. El Líder del DRP, en conjunto con los funcionarios que participaron en la atención del incidente, documentan el incidente e identifican oportunidades de mejoramiento.

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

- h. Se realiza el cierre del incidente, interrupción mayor o evento contingente, y se continúa con la ejecución del procedimiento de acciones preventivas y correctivas del SGSI.

3.4. ACTIVIDADES DE MANEJO DE CRISIS


Actividades y consideraciones necesarias para el manejo de una crisis que afecte o pueda afectar la operación en la atención del cliente interno y externo.

- a. **El P.U. Ingeniero de Sistemas** comunica a la Alta Dirección, teniendo en cuenta los siguientes aspectos:
- ✓ Sistemas y servicios afectados
 - ✓ Resultados del diagnóstico
 - ✓ Acciones realizadas
 - ✓ Tiempo estimado para la normalización
 - ✓ Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles.
 - ✓ Decisiones que debe tomar la alta dirección.
- b. **La Alta Dirección** evalúa la crisis y el impacto que puede tener para prestación de servicios a los usuarios, al igual que define las acciones para afrontar la crisis.
- c. La Alta Dirección, será la única instancia que informará sobre la crisis a nivel interno y externo.

La comunicación de la crisis deberá considerar los siguientes principios:

- ✓ **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis.
- ✓ **Decir la verdad:** Ser honestos en los comunicados, sin embargo no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la ciudadanía. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.
- **Emitir reportes lo más exactos posible:** Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

Los interesados a considerar en la comunicación de la crisis son:

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

- ✓ Funcionarios
- ✓ Contratistas y proveedores
- ✓ Usuarios Externos
- ✓ Ciudadanía en General
- ✓ Gobierno y Autoridades

d. **La Alta Dirección**, o los funcionarios designados por esta, deberá realizar monitoreo permanente de la crisis y tomar las decisiones que correspondan para continuar con la mitigación de la misma.

3.5. ACTIVIDADES DE MANTENIMIENTO

Es responsabilidad del **Líder del DRP**, la actualización del plan y la divulgación de éste a todos los funcionarios involucrados en el proceso.

La actualización y mantenimiento al DRP se debe realizar:

- ✓ Cuando ha transcurrido un año desde la última actualización.
- ✓ Cuando han ocurrido cambios en la plataforma tecnológica objeto del alcance de esta guía.
- ✓ Cuando los resultados de las pruebas requieren actualización del DRP o sus procedimientos.
- ✓ Cuando hay cambios en el personal que operaría el DRP.
- ✓ Cuando los resultados de auditorías así lo indican.

Algunas actividades a realizar para mantener vigente el DRP, son:


3.6. ACTIVIDADES DE PRUEBA

Se deben ejecutar periódicamente actividades de prueba de acuerdo a la programación y metodología especificada en el **Procedimiento de Gestión al Plan de Recuperación ante Desastres**.

Estas pruebas deben incluir:

Escenarios específicos a fallas de:


- ✓ Backup o Respaldo de la información verificación de copias en servidor alternativo
- ✓ Infraestructura de comunicaciones.
- ✓ Infraestructura de bases de datos.

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

- ✓ Infraestructura técnica (servidores)
- ✓ Fallas técnicas en el Centro de Datos.
- ✓ Aplicaciones.

3.7. RECURSOS MINIMOS REQUERIDOS

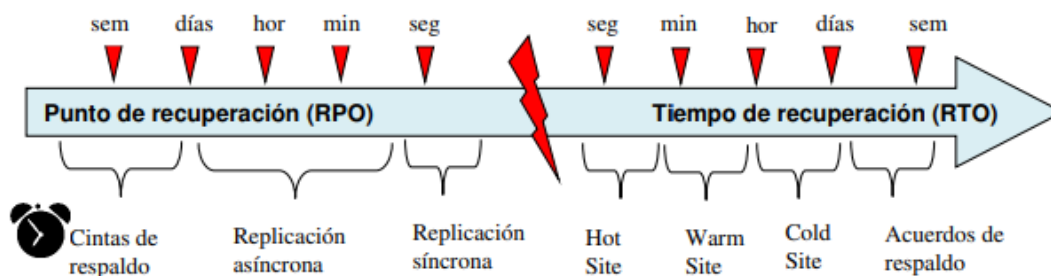
Cantidad	Equipo	Procesador	Memoria	Almacenamiento	Servicios
1	HP ProLiant DL 360 G6	1 Procesador Xeon E5530 2.40 GHz x6 core	6 GB	2 HDD 320 GB	Windows Server 2012 R2 Standard. - Domain Controller (DC), DNS, DHCP.
1	HP ProLiant DL 380 Gen9	10 Procesadores Inter(R) Xeon(R) CPU –E5-2640- V4 – 2.40Ghz x 20 Core	64 GB		Windows Server 2012 R2 Standard. - Microsoft SQL Server 2012. - IIS. - Panacea
1	HP ProLiant DL380 7 (G7)	2 Procesador Intel Xeon x5690 3,47 GHz x12 cores	20 GB	2 HDD 600 GB	Windows Server 2008 R2 Enterprise. - Hyper-V - IIS. - Panacea
1	HP ProLiant DL 380 G9	Intel(R) Xeon(R) E5-2650 2,30 GHz 20 cores	48 GB	4 HDD SAS 600GB	Windows Server 2012 R2 Datacenter. - IIS - Hyper-V

	PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

4. ACTIVIDADES DE RECUPERACIÓN Y CONTINGENCIA

Este plan está basado en el hecho de que por alguna situación crítica interna o externa, no haya acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo o son inaccesibles por completo por un período inaceptable de tiempo. Las estrategias para seguir serán acordes a la magnitud y duración tentativa del incidente y se deberán tomar en cuenta los siguientes aspectos:

- Evaluación de los daños
- Evaluación del tiempo estimado de la recuperación
- Análisis exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo con el tipo de incidente.




Este plan solo podrá ser activado únicamente cuando el área Directiva en compañía del área de gerencia de la información sea aprobada

Para la recuperación de la contingencia el P.U ingeniero de sistemas definirá el servidor en el cual se activará el rol de hypervisor para la instalación de máquinas virtuales las cuales están almacenadas en backup que mantiene el área

El proceso de gerencia de la información debe garantizar un servidor con el rol alternativo de hypervisor para el caso de activar una contingencia con las características necesarias

Estrategia de acción

 <p>HOSPITAL DEL SUR ITAGÜÍ</p>	<p>PLAN DE RECUPERACIÓN ANTE DESASTRES – DRP</p>	Código:
		Versión: 1
		Fecha Actualización:
		Elaborado Por:

Las estrategias y planes de acción considerados para la recuperación del desastre, han sido orientados a cubrir cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal a la institución donde se ubica el centro de cómputo o bien a los servicios de cómputo y telecomunicaciones en que se apoyan las todas aplicaciones críticas de la entidad, las cuales se definieron como:

1. Servidor URANO (BASES DE DATOS)
2. Servidor BASES DATOS CNT
3. Servidor DOMINIO - MARTE
4. Servidor Svrintranet
5. Servidor terminal- Neptuno
6. Servidor svrprincipal
7. Sevidor Jupite
9. Servidor Pluton
10. Servidor Kryton
- 1

La decisión para desarrollar este plan, se basó en las características de la operación actual de la entidad, así como el nivel de dependencia de tecnología de información y comunicaciones.