CONTENIDO

INTRODUCCIÓN

El plan de contingencia de la gestión de información y las tecnologías de la E.S.E Hospital Local de Piedecuesta, es un documento que establece los lineamientos y respuestas para atender en forma oportuna, ante la posible pérdida, destrucción o robo de la información.
Tanto el Hardware como el Software están expuestos a diversos Factores de Riesgo Humano y Físico. Pueden originarse pérdidas de información catastróficas, bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que pueden producir daño físico irreparable.

El área de sistemas tiene el propósito de proteger la información y asegurar que el desarrollo de las funciones de la institución no se vea afectada ante un evento catastrófico.

Para ello es importante contar con un plan de contingencia que ayude a recobrar y restablecer rápidamente la marcha normal de los procesos de la institución.

1. **GENERALIDADES**

1.1 Objetivos

1.1.1 Objetivo General

Formular un Plan de Contingencia que permita asegurar y restaurar la información en caso de un evento informático catastrófico, con las menores pérdidas posibles, en forma rápida, eficiente y oportuna; asegurando la continuidad en los procedimientos de la E.S.E Hospital Local de Piedecuesta.

1.1.2 Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en la E.S.E Hospital Local de Piedecuesta.
- Establecer los niveles de complejidad de las fallas del sistema y los posibles tiempos de no disponibilidad de los diferentes softwares.

1.2 Alcance

El Plan de Contingencia Informático está basado en la realidad que manifiesta la E.S.E Hospital Local de Piedecuesta, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

2. **Responsables**

Ingeniero de sistemas

3. **Definiciones**

AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

CONTIGENCIA: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

ELEMENTOS EN RIESGO: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos ante la eventualidad que lo afecte de forma parcial o total.

4. ANALISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

4.1 Factores que afectan la seguridad física y la infraestructura.

Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales. Ambos riesgos tienen su origen de causas externas a la institución y su grado de previsión es muy mínimo. La probabilidad de origen natural es baja, mientras, que los riesgos artificiales son de probabilidad media.
De igual forma se encuentran las descargas o cortes eléctricos, los cuales pueden generar interrupción y afectar la atención a los usuarios.

Para la clasificación de los activos de la tecnología informática de la institución se han considerado tres criterios:

- **Grado de negatividad:** Un evento se define con grado de negatividad (Leve, moderado, grave y muy severo).

- **Probabilidad de ocurrencia**:

CONCEPTO	DEFINICIÓN	VALOR
FRECUENTE	Puede ocurrir dentro de un breve período, varias veces en un año.	4
OCASIONAL	Es probable que ocurra 1 a 2 veces por año.	3
RARO	Es posible que ocurra alguna vez en 2 a 5 años.	2
REMOTO	Puede ocurrir alguna vez en 5 a 30 años.	1

- **Impacto**

IMPACTO	VALORACIÓN	CRITERIO
Insignificante	1	Pérdida de control, operaciones, Información y/o equipamiento no sensibles.
Moderado	2	Pérdida de control, operaciones, Información y/o equipamiento medianamente sensibles
Mayor	3	Pérdida de control, operaciones, Información y/o equipamiento medianamente sensibles que pueden causar retraso o interrupción de servicios.
Catastrófico	4	Pérdida de control, operaciones, Información y/o equipamiento críticos que puede causar daño serio de infraestructura o destrozo patrimonial

4.2 Clases de riesgo

- Incendio
- Robo común de equipos y archivos
- Falla en los equipos
- Acción de virus informático
- Fenómenos naturales
- Accesos no autorizados

4.3 Minimizar el Riesgo

Corresponde al plan de contingencia informático minimizar los riesgos tomando medidas preventivas y correctivas sobre cada uno.

4.3.1 Incendio

Grado de negatividad: Muy Severo
Frecuencia de evento: Raro
Grado de impacto: Catastrofico

Acciones Preventivas:	**Acciones Correctivas**
• Ubicar extintores cerca de los cuartos de telecomunicaciones donde se encuentra los servidores y dispositivos tecnológicos. • Ejecutar programas de capacitaciones sobre el uso de elementos de seguridad y primeros auxilios. • Realizar copias de seguridad de los servidores y equipos de escritorio del personal administrativo y jefes de enfermería • Ubicar los servidores en diferentes cuartos.	• Si en caso de incendio el servidor queda afectado se procede a restaurar la copia de seguridad más reciente en el servidor de respaldo que debe encontrarse en otra ubicación. • En las oficinas apagar el fuego con el extintor más cercano. • Suministrar un equipo de repuesto y restaurar la copia de seguridad más reciente en caso de daño en el equipo.

Analizando el riesgo de incendio, es necesario ubicar los servidores en lugares estratégicamente distantes y cercanos a los extintores, para en caso de emergencia sea más fácil controlar el fuego y proteger los dispositivos de almacenamiento.

4.3.2 Robo común de equipos y archivos

Grado de negatividad: Grave
Frecuencia de evento: Raro
Grado de impacto: Mayor

Acciones Preventivas:	**Acciones Correctivas**
• Llevar registro de los objetos que salen de la institución por parte del personal de vigilancia. • Autorización escrita firmada por coordinador del área o el responsable para salidas de equipos.	• Suministrar un equipo de repuesto con el fin de no interrumpir los procesos, restaurando la copia de seguridad más reciente, que se encuentra debidamente alojada en la nube.

4.3.3 Falla en los equipos

Grado de negatividad: Grave
Frecuencia de evento: Raro
Grado de impacto: Moderado

Acciones Preventivas:	**Acciones Correctivas**
• Incluir todos los equipos de la E.S.E Hospital Local de Piedecuesta en un plan de mantenimiento preventivo, con el fin de reducir el riesgo de fallas y aumentar la vida útil de los mismos. • Contar con un stock de repuesto para el reemplazo de estos en caso de daño. • Usar ups en cada estación de trabajo en caso de fallas en la energía eléctrica.	• Reparar las fallas que se presenten en el menor tiempo posible. • Suministrar un equipo de repuesto para el normal desempeño del usuario en su área de trabajo. • Restaurar la copia de seguridad más reciente.

4.3.4 Acción de virus informático

Grado de negatividad: Moderado
Frecuencia de evento: Ocasional
Grado de impacto: Mayor

Acciones Preventivas:	**Acciones Correctivas**
• Mantener actualizado el antivirus en cada estación de trabajo • Ingresar los usuarios a un dominio con el fin de restringir permisos para instalación de software no autorizado. • Configurar router mikrotik para evitar acceso a sitios no autorizados en la web. • Adquirir firewall para proteger los equipos contra accesos no deseados.	• Hacer la eliminación del virus si es posible, de lo contrario formatear y hacer una nueva instalación del sistema operativo • Suministrar un equipo de repuesto para evitar la interrupción de las labores o prestación del servicio. • Si el equipo corresponde a personal administrativo o jefe de enfermería realizar la restauración de la información ingresando a la cuenta de nextcloud de cada usuario.

	• Utilizar servidor de respaldo en caso de infección en el servidor que se encuentra en producción.

4.3.5 Fenómenos Naturales

Grado de negatividad: grave
Frecuencia de evento: remoto
Grado de impacto: Catastrófico

Acciones Preventivas:	**Acciones Correctivas**
• Ubicar los servidores en espacios seguros libres de filtraciones y en posición tal que ante un movimiento telúrico no sufra una caída que pueda averiar el equipo. • Ubicar los servidores en lugares estratégicos en espacios separados.	Si los equipos sufren daño físico • Proceder a tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. • Recoger los respaldos de datos, programas, manuales y claves del lugar en donde se encuentren reguardados. • Instalar el sistema operativo. • Restaurar la información de las bases de datos y programas. • Revisar y probar la integridad de los datos.

4.3.6 Accesos no autorizados

Grado de negatividad: grave
Frecuencia de evento: remoto
Grado de impacto: Mayor

Acciones Preventivas:	**Acciones Correctivas**
• Realizar cambio periódico de claves de acceso • Desactivar el usuario en el sistema cuando el colaborador se retira de la institución. • Capacitar y socializar a los colaboradores sobre la importancia de la	• Detección del incidente • Desconectar los equipos de la red • Iniciar un proceso de valoración para determinar las posibles consecuencias e impacto • Cambiar contraseñas

confidencialidad de sus claves de acceso y el hábito de cambiarlas periódicamente. • Asignar a los colaboradores únicamente el perfil en el sistema de acuerdo a su rol y actividades a desempeñar. • Adquirir firewall para controlar el acceso a internet y posibles ataques que pueda afectar la información.	• Salvar la información de los servidores. • Bloquear las direcciones IP si es necesario. • Implantar las medidas técnicas de recuperación (backup de los sistemas, copias de seguridad)

5 CONCLUSIONES

El resguardo de la información y la continuidad de las operaciones ante eventualidades o desastres, constituye una de las principales estrategias que deben desarrollar y procurar las organizaciones modernas ya sean públicas o privadas, ya que de ello depende en la mayoría de los casos la continuidad o cese de los servicios entregados por la organización a la comunidad.

El presente Plan de contingencias y Seguridad de la Información, tiene como objetivo principal proteger la infraestructura de la Red y los Sistemas de Información, tomando las medidas de seguridad pertinentes ante una contingencia de cualquier tipo y llevar un proceso de recuperación de la información y las actividades laborales en el menor tiempo posible.