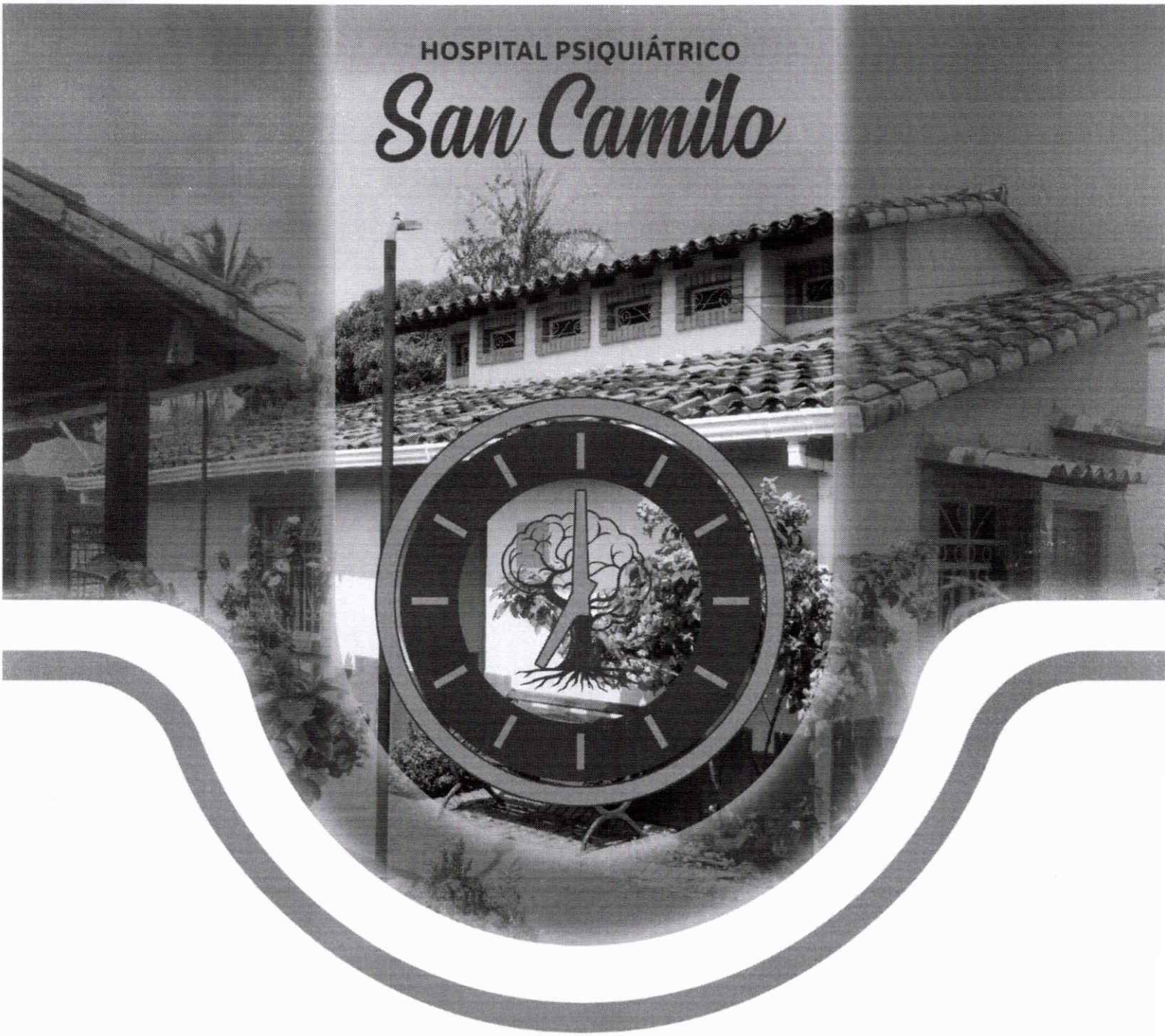

PLAN DE CONTINGENCIA ESE HOSPITAL PSIQUITRICO SAN CAMILO Y SEDE

Tipo de proceso: **ADMINISTRATIVO**

Proceso: **INFORMACION Y TECNOLOGIA**

Subproceso: **TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN TIC**

Código: **AD-GIT-TIC-PL-03**

Versión: **02**

Fecha de aprobación: **30 ENERO 2025**

TABLA DE CONTENIDO

N500

1. INTRODUCCIÓN

Para realizar el Plan de contingencia del área de TIC de la E.S.E. Hospital Psiquiátrico San Camilo se tiene en cuenta la información como uno de los activos más importantes de la organización, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la entidad. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con los diferentes sistemas de la institución (entrada de datos, generación de reportes, consultas, etc.).El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera se establecerán medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es importante resaltar que para que la institución logre sus objetivos es indispensable el manejo de información, por tanto, necesita garantizar tiempos de indisponibilidad mínimos para no originar distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación, ya que de continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar los servicios y programas por falta de información para el control y toma de decisiones de la entidad. De acuerdo a lo anterior es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea el menor posible.

2. JUSTIFICACIÓN

El siguiente documento tiene como finalidad mitigar los riesgos potenciales a los cuales está expuesta la institución en cuanto al manejo de los procesos y resguardo de la información.

Con el planteamiento propuesto en este documento, el proceso de Gestión de la información, contará con un instrumento que permita a la institución y a las áreas encargadas de la información la toma de decisiones y acciones a ejercer, para garantizar la continuidad en la prestación de los servicios y así mismo minimizar los riesgos a los que se puede presentar la ESE Hospital Psiquiátrico San Camilo en una contingencia.

3. OBJETIVO GENERAL

Establecer de forma clara las acciones a realizar, para responder a posibles riesgos ante fallas, en caso de producirse un acontecimiento intencionado o accidental que degrada los recursos informáticos o físicos de la institución, con el fin de estar preparados para reactivar los servicios en el menor tiempo posible y generar el menor impacto en la atención de los pacientes y usuarios finales.

3.1 Objetivos Específicos

- Definir actividades de planeación, alistamiento y ejecución de actividades enfocadas en la protección de la información, contra daños producidos por corte en los servicios, fenómenos naturales o humanos.
- Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.
- Mantener copias de seguridad o BackUp en discos externos, con el fin de salvaguardar la información más importante de cada uno de los servidores de la entidad.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

4. PARTES INTERESADAS

Este instructivo aplica para todo el personal de las áreas Médico, asistencial y administrativo del Hospital Psiquiátrico San Camilo y sus sedes.

5. POLÍTICAS

- El cumplimiento de este Plan de Contingencia involucra a todo el personal de la institución, con el fin de que las diferentes áreas garanticen la continuidad en la prestación de los servicios.
- Se debe asegurar el uso correcto de los formatos establecidos por la institución en donde se hará el registro de la información durante la contingencia y una vez esta culmine sean entregados al área correspondiente para su resguardo.

6. PROCESOS RELACIONADOS

- Aplica para todos los procesos de la institución.

7. REQUISITOS LEGALES APLICABLES

- Ley 594 de 2000, ley general de archivos.
- Decreto 2609 de 2012, Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades. Capítulo IV, la gestión de documentos electrónicos de archivos.
- Acuerdo 050 de 2000 "Por el cual se desarrolla el artículo 64 del título VII "conservación de documento", del Reglamento general de archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo".

8. DESCRIPCIÓN DEL PLAN

8.1 Identificación De Procesos Y Servicios

Principales Procesos de Software Identificados:

SOFTWARE:
- SO MICROSOFT WINDOWS SERVER 2008
- MIKROTIK
- SAHI
- SALUD 360
- Facturación electrónica
- MAT
- Gestor de Solicitudes
- San Camilo Learnig

- Nomina
- Juliana
- Ingreso
- PW – Análisis
- PSG – Análisis

Tabla 1. SOFTWARE

SOFTWARE BASE
– SQL SERVER.
– Back Up de la Información.
– Ejecutables de las aplicaciones.

Tabla 2. SOFTWARE BASE

RESPALDO DE LA INFORMACIÓN
– Back Up de la Base de Datos SAHI
– Back Up de la Plataforma SIGED
– Back Up de los Servidores.

Tabla 3. RESPALDO DE LA INFORMACIÓN

8.2 Análisis De Evaluación De Riesgos Y Estrategias

Metodología aplicada: Para la clasificación de los activos de Tecnologías de Información de la E.S.E. Hospital Psiquiátrico San Camilo se ha considerado tres criterios:

Grado de negatividad: En un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).

Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo).

Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de Contingencia: Son procedimientos que definen cómo una entidad dará continuidad o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

Leves: Caídas de energía de corta duración, fallas en disco duro, etc.)

Severas: Destrucción de equipos, incendios, etc.)

Riesgo: Es la vulnerabilidad de un Activo o bien, ante un posible potencial de perjuicio o daño. A continuación, se definen los riesgos que existen

Riesgos Naturales: Tales como mal tiempo, terremotos, inundaciones, etc.

Riesgos Tecnológicos: Tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

Riesgos Sociales: Hace referencia a actos terroristas y desórdenes.

Activos susceptibles de daño

Hardware

Software y utilitarios

Datos e información

Documentación

Suministro de energía eléctrica

Suministro de telecomunicaciones

Posibles Daños

Acceso denegado a los recursos informáticos, ya sea por cambios involuntarios o intencionales, tales como: cambio de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

Fuentes de daño

Desastres Naturales (Movimientos telúricos, inundaciones, fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no condicionamiento atmosférico necesario).
Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red, Switch, cableado de la Red, Router, Firewalls).

Tabla 4. Fuentes de daño

Clases de Riesgos

• Robo común de equipos y archivos
• Falla en los equipos
• Equivocaciones
• Acción virus informático

• Fenómenos naturales
• Accesos no autorizados
• Ausencia del personal de sistemas.

Tabla 5. Clases de Riesgos

8.3 Eventos Considerados Para El Plan De Contingencia

Cuando se efectúa un riesgo, este puede producir un Evento, por tanto, a continuación, se describen los eventos a considerar dentro del Plan de Contingencia.

Corte General del Fluido eléctrico

1. Si se presenta un cortocircuito, la UPS mantendrá activo los servidores, mientras se repara la falla eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia).
3. En caso de no responder la UPS, ingresa la planta eléctrica (tiempo máximo 15 Seg) en caso que la planta no responde, para mantener el tiempo de respaldo de la UPS se procede a apagar los dispositivos fundamentales.
4. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de UPS a corriente normal (corriente brindad por la empresa eléctrica).

Indisponibilidad Del Centro De Cómputo:

Destrucción del centro de cómputo

1. Contar con el inventario total de sistemas actualizado.
2. Identificar recursos de hardware y software que se puedan rescatar.
3. Salvaguardar los Back Up de información realizada.
4. Identificar un nuevo espacio para restaurar el Centro de Cómputo.
5. Presupuestar la adquisición de software, hardware, materiales, personal y transporte.
6. Adquisición de recursos de software, hardware, materiales y contratación de personal.
7. Iniciar con la instalación y configuración del nuevo centro de cómputo.
8. Restablecer los Back Up realizados a los sistemas.

Perdida de servicio internet

1. Realizar pruebas para identificar posibles problemas dentro de la entidad.
2. Si se evidencia problema en el hardware, se procederá a cambiar el componente.

3. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor.
4. Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
5. Si el daño es por parte del proveedor que suministra el servicio, se debe validar tiempo en restablecerse.
6. Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
7. Realizar pruebas de operatividad del servicio.
8. Servicio de internet activo.

Daño en Base de Datos

1. Verificar el daño ocurrido en la información.
2. Se restaura la Base de Datos con la copia a corte de ocurrido el evento.
3. Verificar la información con los usuarios.

Capacidad de Almacenamiento en los Servidores:

1. Hacer mantenimiento de temporales, Logs, pasar los Back Up que se estén realizando a otro dispositivo.
2. Realizar depuración de la información almacenada en los discos.
3. Estudiar la opción de una solución NAS, para aumentar el almacenamiento.

8.4 Minimización Del Riesgo

Teniendo en cuenta lo anterior, corresponde al Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo.

Incendio o Fuego

Grado de Negatividad: Muy Severo
Frecuencia de Evento: Aleatorio
Grado de Impacto: Alto

Situación Actual	Acción Correctiva
• La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso	• Se cumple

Situación Actual	Acción Correctiva
cuenta con un extintor debidamente cargado.	
• El servidor realiza Back Up de la información cada 24 horas según programación y se retira los Back Up semanalmente.	• Realizar Back Up del servidor de forma diaria, almacenada en disco duros externos y ubicarlos estratégicamente cerca de la salida principal de la institución. • Las copias deben ser resguardadas en un lugar externo a la institución.

Tabla 6: Incendio o fuego

Robo Común de Equipos y Archivos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Moderado

Situación Actual	Acción Correctiva
Autorización escrita firmada por el Coordinador área de Almacén y funcionario responsable, para la salida de equipos de la institución.	Se cumple por medio del formato establecido para salida de equipos.

Tabla 7: Robo común de equipos

Falla en los Equipos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Grave

Situación Actual	Acción Correctiva

La falla en los equipos muchas veces se debe a falta de mantenimiento, limpieza y a mal uso por parte de los usuarios.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año. Realizar Capacitaciones del uso adecuado de los equipos.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen de protección para descargas eléctricas	No se cumple, la institución no cuenta con una red eléctrica regulada al 100% y no cuenta con UPS para cada equipo de cómputo.
Pérdida de Información, por no existir una copia de seguridad.	Contar con un servidor de archivos(en la nube, servidor físico, discó externo)

Tabla 8: Falla en los equipos

Acción de Virus Informático

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Continuo

Grado de Impacto: Grave

Situación Actual	**Acción Correctiva**
Se cuenta con un software antivirus para la entidad y su actualización se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación de las licencias antivirus.
Únicamente el área de TIC es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple.
Se tiene acceso restringido al servidor, únicamente es el Coordinador de Sistemas el encargado de cambiar configuraciones y anexar nuevos equipos.	Antes de loguearse una máquina a la red, se debe comprobar la existencia de anti-virus en la misma.
Por medio del correo electrónico se obtienen virus constantemente.	Crear un correo institucional para cada funcionario por medio de la página Web, de forma que

Situación Actual	Acción Correctiva
	únicamente se reciba información de importancia para la entidad.
Los antivirus se actualizan automáticamente en cada equipo.	Se cumple

Tabla 9: Acción de virus informático

Riesgos para la seguridad de la información

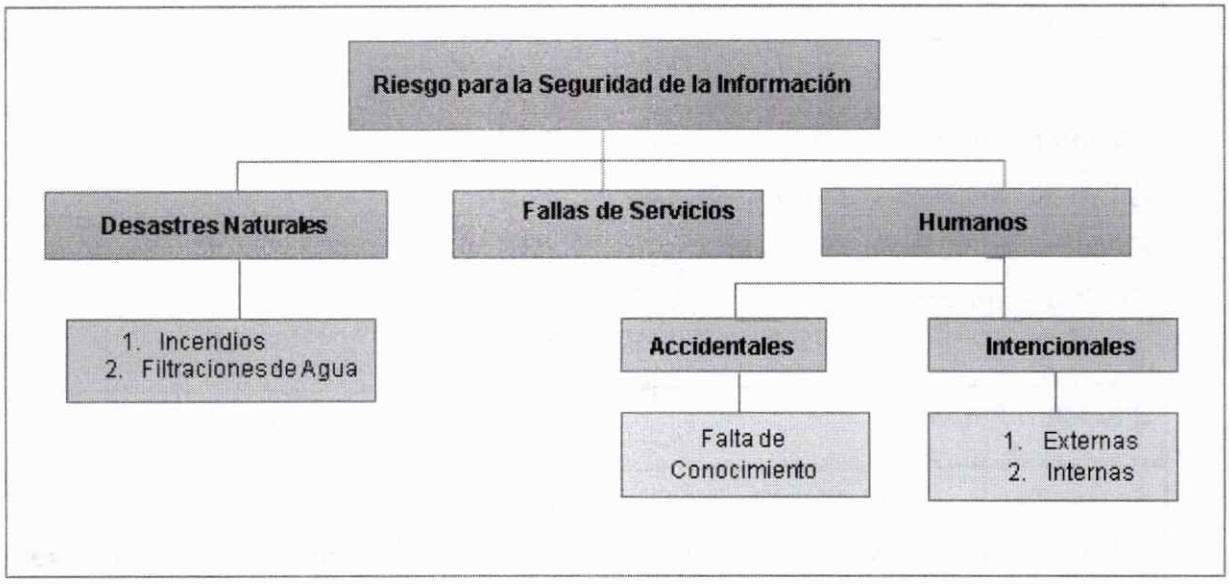

Imagen 1. Riesgos seguridad de la información

Riesgos Por Naturaleza Física

FÍSICOS	Ruido, Iluminación, Cambios de Temperaturas, Humedad, Ventilación
INCENDIO	Incendio de sólidos, Incendios de líquidos, Incendios de Gases, Incendios eléctricos, Incendios combinados
PSICOSOCIALES	Repetitividad, Sobre tiempo, Atención al público, Estrés individual, Estrés organizacional, Factores de condiciones de trabajo, Alteraciones psicosomáticas asociadas

Tabla 10: Riesgo por naturaleza física

Riesgos Ambientales

Los riesgos ambientales a los que se ven expuestos los archivistas manejan una gran cantidad de variantes ya que se refieren al entorno ambiental en el que interactúan a diario y que se generan ya sea por el medio ambiente, la ubicación geográfica y los elementos que lo rodean.

Temperaturas
Humedad relativa
La luz
Contaminantes Atmosféricos
polvo y polución
Manejo de Objetos Pesados
Estrés y carga laboral

Tabla 11: Riesgos ambientales

Accesos No Autorizados

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Situación Actual	**Acción Correctiva**
Se controla el acceso a los sistemas de información, mediante la definición de un administrador con su respectiva clave.	Se cumple
La asignación de usuario se realiza bajo criterio del Administrador del Sistema encargado de cada aplicativo y se solicita por parte del jefe de área.	Se cumple.
La oficina administrativa no comunica al área de TIC, cuando un funcionario sale a vacaciones o se retira de la entidad a fin de desactivar ese usuario.	Se debe informar al administrador del sistema, que funcionario sale a vacaciones, con el fin de bloquear el usuario a los diferentes aplicativos por el tiempo de ausencia, igualmente en caso de retiro definitivo.

Situación Actual	Acción Correctiva
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	- Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software. - El administrador de cada sistema encargado de la creación de usuarios hace entrega del formato con las indicaciones y recomendaciones sobre el uso de su clave y de la información a cargo.

Tabla 12: Accesos no autorizados

8.5 Plan de recuperación y respaldo de la información:

Con el objetivo de dar respuesta inmediata que interrumpan la operación normal de los servicios de cómputo, se definen las siguientes actividades:

- Previas al Desastre.
- Durante el Desastre.
- Después del Desastre.

Actividades previas al desastre

Estas actividades deben ser efectuadas como parte de una rutina diaria, que permitan enfrentar cualquier incidente y minimizar los riesgos e impactos que el evento pudiese causar, las cuales se detallan a continuación:

a. Sistemas de Información

- Relacionar los Sistemas de Información del hospital, tanto los de desarrollo propio, como los desarrollados por empresas externas.
- Contar con la configuración correspondiente requerida para la operatividad de cada sistema, tales como (Manuales técnicos, arquitectura de software, direccionamiento, servicios web y puertos habilitados).

- Mantener actualizado la información de los proveedores prestadores de servicios informáticos.
- Contar con el respectivo plan de contingencia y plan de Back Up a los proveedores de software externos.

b. Equipos de Cómputo

- Se debe tener en cuenta el inventario de Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).
- Emplear los siguientes criterios sobre identificación y protección de equipos:

1. Garantía de los dispositivos adquiridos en la institución.
2. Señalización o etiquetamiento de los equipos para su distribución en el inventario.
3. Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Back Up)

Se sigue el procedimiento de copias de seguridad de la información, validando cada uno de puntos necesarios para la correcta ejecución de los aplicativos en la institución. Las copias de seguridad son las siguientes:

1. Back Up de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución de los aplicativos de la institución). El proceso de ejecución de copias se realiza diariamente de forma automática y semanalmente de forma manual.
2. Back Up del Sistema Operativo: Todas las versiones del sistema operativo instalados en la Red. (Periodicidad – Semestral).

8.6 Contingencia, Respaldo Y Continuidad De Procesos Críticos

Con el fin de brindar continuidad en los sistemas de información, así como en los demás servicios que realizan procesos críticos se definen las siguientes actividades:

a. Mantener actualizados los formatos en físico más relevantes de los procesos administrativos y asistenciales (servicios de hospitalización y ambulatorio), para garantizar el adecuado registro clínico o administrativo esto cuando el hospital no cuente con el sistema de información institucional. Una vez culminado el plan de contingencia, cada servicio del hospital realiza la entrega de los documentos a las áreas que correspondan y al área de archivo las historias de los pacientes para su respectiva custodia.

b. En cada servicio asistencial se contará con un paquete impreso de los formatos requeridos para el registro de la Historia Clínica, esta carpeta contiene los formatos impresos y será revisada y actualizada al menos una (1) vez al año.
c. El coordinador y/o Líder de área debe garantizar que el personal conozca el proceso a realizar en una contingencia.

Documentos a utilizar en la contingencia de acuerdo al servicio asistencia y según su necesidad:

Nombre del Documento
Registros de medicamentos
Consulta médica
Evolución médica
Orden de Medicamentos
Orden de Procedimientos
Nota de enfermería
Justificación de medicamentos No Pos
Justificación de procedimientos No Pos
Epicrisis
Incapacidad medica

Tabla 13: Documentos contingencia

Tiempos y responsable para activación de la contingencia:

La activación del Plan de Contingencia será realizada exclusivamente por el Subdirector Administrativo y Financiero, quien emitirá un comunicado oficial dirigido a todos los servicios asistenciales y administrativos, informando el inicio de la contingencia, el alcance del evento y las acciones inmediatas a ejecutar.

Tiempos de activación según el servicio:

- Consulta externa y servicio de urgencias: La contingencia será activada transcurridos 30 minutos de falla en el sistema HCE.
- Servicios hospitalarios: La contingencia será activada transcurridos 45 minutos de falla en el sistema HCE.

Nota: En caso de presentarse una emergencia clínica, el Plan de Contingencia deberá ser activado de forma inmediata, sin esperar los tiempos establecidos. El Subdirector Administrativo y Financiero deberá emitir el comunicado oficial correspondiente e informar

oportunamente a todo el equipo asistencial y administrativo para garantizar la continuidad del servicio y el registro oportuno de la información clínica.

Antes de iniciar la contingencia:

Tener en cuenta:

- Indicar al personal del servicio la ubicación donde se encuentran resguardados los archivos a utilizar.

- Se debe contar con suficientes registros físicos requeridos para consignar la información de ingreso y atención dada al paciente en caso de falla del fluido eléctrico, ausencia del sistema de información.

Durante la Contingencia:

- Realizar los registros necesarios del proceso de atención médico asistencial (hospitalización y ambulatorio) en los formatos definidos para cada proceso.
- La parte administrativa y financiera realiza los registros manuales en los formatos definidos por sus líderes de área.

Finalizada la contingencia:

- Una vez se supera el inconveniente presentado, en el área asistencial los coordinadores de enfermería deben organizar por paciente la carpeta con los documentos diligenciados y entregarlos al área de archivo para su respectivo resguardo.
- Las órdenes tanto de medicamentos, procedimientos o laboratorio clínicos, una vez culmine la contingencia el personal médico debe registrar esta información en el sistema, con el fin de que el área de farmacia pueda hacer el descargue de los medicamentos e insumos en el sistema y así el área de facturación genere la venta y factura correspondiente a cada paciente.

8.7 Conceptos Generales

Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

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. En el caso de los datos de una organización, la privacidad y la

seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

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. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que, además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Incidente o Evento

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

8.8 Plan De Actividades

Con el fin de hacer seguimiento y cumplir a cabalidad con lo establecido en el Plan de Contingencia se definen las siguientes actividades que complementan los diferentes procesos manejados en la ESE Hospital Psiquiátrico San Camilo:

Anexo Cronograma

Cronograma de Actividades Código: ES - GIM -GIC - P- 11 - R -01.

9. SEGUIMIENTO Y EVALUACIÓN

El seguimiento al plan de contingencia del Hospital Psiquiátrico San Camilo se realizará de forma trimestral realizando reuniones con los líderes de cada una de las áreas que hacen parte del equipo de gerencia de la información.

La evaluación del Plan de Contingencia tiene como objetivo determinar el nivel de cumplimiento, eficacia y oportunidad en la activación, ejecución y restablecimiento de los servicios críticos durante un evento simulado o real, garantizando la continuidad de la atención y la protección de la información institucional, especialmente la relacionada con el sistema HCE.

Metodología de Evaluación

La evaluación se realizará una vez finalizado el simulacro o el evento real, aplicando:

- Listas de verificación por servicio.
- Revisión de evidencias documentales y técnicas.
- Entrevistas con responsables.
- Observación directa del desempeño del personal.
- Registro cronológico del evento (bitácora).
- Análisis de tiempos de restablecimiento.

Los evaluadores designados deberán consolidar la información para generar conclusiones y definir acciones de mejora.

Los documentos que se maneja para hacer seguimiento al finalizar cada ejercicio o en el evento real, que deberán generarse son:

- Acta del simulacro
- Informe técnico del área TIC
- Informe post-simulacro consolidado
- Plan de mejora con responsables y fechas
- Evidencias físicas y digitales organizadas en expediente del simulacro
- Acta de reunión con los líderes de área y compromisos adquiridos.

- Seguimiento a las actividades que se encuentran relacionadas en el plan de contingencia de TIC.
- Tabla de Evaluación del Simulacro del Plan de Contingencia (anexo al plan)

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ing. Erwing Jesid Dávila Garcia **Web Máster**		
Juan Gabriel Rojas Gómez **Coordinador de Gestión Documental.**	Edgar Albarracín Cogollo **Subdirector Administrativo y Financiero**	Natalia Sofia Ojeda Ortiz **Gerente**
FECHA: 30/01/2025	FECHA: 30/01/2025	FECHA: 30/01/2025