Tipo de proceso: PLAN DE CONTINGENCIA

Proceso: Gestión de la Información

Subproceso: Tecnologías de la información y comunicaciones

Código: AD-GIT-TIC-PL-03

Versión: 03

Fecha de aprobación: 14/01/2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4

2. JUSTIFICACIÓN 5

3. OBJETIVO GENERAL 5

3.1 Objetivos Específicos 5

4. ALCANCE 6

4.1 Enfoque diferencial 6

5. TALENTO HUMANO 6

6. PARTES INTERESADAS 6

7. POLÍTICAS 7

8. PROCESOS RELACIONADOS 7

9. REQUISITOS LEGALES APLICABLES 7

10. DESCRIPCIÓN DEL PLAN 8

10.1 Identificación de procesos y servicios 8

10.2 Análisis de evaluación de riesgos y estrategias 9

10.2.1 Posibles Daños 10

10.3 Eventos considerados para el plan de contingencia 10

10.3.1 Corte General del Fluido eléctrico 10

10.3.2 Indisponibilidad Del Centro De Cómputo: 11

10.3.2.1 Destrucción del centro de cómputo 11

10.3.2.2 Perdida de servicio internet 11

10.3.2.3 Daño en Base de Datos 11

10.3.2.4 Capacidad de Almacenamiento en los Servidores: 12

10.4 Minimización del riesgo 12

10.4.1 Incendio o Fuego 12

10.4.2 Robo Común de Equipos y Archivos 13

10.4.3 Falla en los Equipos 13

10.4.4 Acción de Virus Informático 13

10.4.5 Riesgos para la seguridad de la información 14

10.4.5.1 Riesgos Por Naturaleza Física 15

10.4.5.2 Riesgos Ambientales 15

10.4.6 Accesos No Autorizados 15
10.5 Plan de recuperación y respaldo de la información: 16
10.5.1 Actividades previas al desastre 16
10.6 Contingencia, respaldo y continuidad de procesos críticos 17
10.6.1 Tiempos para activación de la contingencia: 18
10.*6.1.1 Antes de iniciar la contingencia:* 19
10.6.1.2 Durante la Contingencia: 19
10.6.1.3 Finalizada la contingencia: 19
10.7 Conceptos generales 19
10.8 Plan de actividades 21
11. SEGUIMIENTO Y EVALUACIÓN 21

1. INTRODUCCIÓN

Para realizar el Plan de contingencia del área de TIC de la E.S.E. Hospital Psiquiátrico San Camilo y sedes 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 y sedes 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. ALCANCE

El Plan de Contingencias de la ESE Hospital Psiquiátrico San Camilo y sedes establece los lineamientos y procedimientos necesarios para garantizar la continuidad operativa de los servicios de salud mental ante eventos disruptivos, internos o externos, que puedan afectar la infraestructura, los sistemas de información, los procesos administrativos o la prestación de atención clínica. Su alcance incluye la identificación de riesgos, la definición de planes de respaldo, recuperación de información, protocolos de comunicación, roles y responsabilidades del personal, así como la coordinación con las sedes y áreas funcionales de la entidad, asegurando la protección de los recursos institucionales y la prestación continua de los servicios esenciales.

4.1 Enfoque diferencial

El Plan de Contingencias incorpora un enfoque diferencial, orientado a garantizar que las medidas de continuidad y recuperación consideren las necesidades de todos los usuarios del hospital y del personal administrativo. Esto asegura que los procedimientos de emergencia, comunicación y acceso a los servicios se implementen de manera equitativa, segura y centrada en el usuario, minimizando el impacto de los eventos críticos sobre la atención y la operación institucional.

5. TALENTO HUMANO

El Plan de Contingencias considera al talento humano como un recurso estratégico para garantizar la continuidad operativa de la ESE Hospital Psiquiátrico San Camilo y sedes. Incluye la definición de roles y responsabilidades frente a situaciones de emergencia, la capacitación permanente en protocolos de contingencia, gestión de riesgos y uso de sistemas críticos, así como la apropiación tecnológica del personal administrativo y clínico, asegurando que estén preparados para actuar de manera coordinada y eficiente ante eventos que puedan afectar los procesos institucionales.

6. PARTES INTERESADAS

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

7. 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.

8. PROCESOS RELACIONADOS

- Aplica para todos los procesos de la institución.

9. REQUISITOS LEGALES APLICABLES

- **Ley 594 de 2000**, ley general de archivos. Regula la organización y funcionamiento de los archivos en Colombia, establece obligaciones para las entidades públicas en la gestión integral de documentos durante todo su ciclo vital, independientemente del soporte. Aplica para todos los procesos archivísticos, incluyendo documentos físicos y electrónicos, y es la base de la gestión documental institucional.
- **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.
- **Decreto 2578 de 2012 – Sistema Nacional de Archivos** Establece el Sistema Nacional de Archivos y la Red Nacional de Archivos, definiendo las responsabilidades de las entidades públicas en la organización, conservación y consulta de documentos. Aplica directamente en la estructuración del área de gestión documental dentro de la ESE Hospital Psiquiátrico San Camilo y sus sedes.
- **Decreto 1080 de 2015 – Decreto Único Reglamentario del Sector Cultura y Gestión Documental,** Esta versión incorpora las modificaciones introducidas al Decreto Único Reglamentario del Sector Cultura a partir de la fecha de su expedición.
- **Acuerdo 02 de 2021 – Archivo General de la Nación** Sustituye el Acuerdo 050 de 2000 y establece los lineamientos actuales para la prevención del deterioro de documentos, situaciones de riesgo documental y conservación de archivos

institucionales. Es obligatorio para todas las entidades públicas y garantiza la protección y continuidad de la información durante eventos críticos.

10. DESCRIPCIÓN DEL PLAN

10.1 Identificación de procesos y servicios

Tabla 1. Principales Procesos de Software Identificados:

SOFTWARE:
- SO MICROSOFT WINDOWS SERVER 2008
- MIKROTIK
- SAHI
- Facturación electrónica
- MAT
- Gestor de Solicitudes
- San Camilo Learnig
- Nomina
- Juliana
- Ingreso
- PW – Análisis
- PSG – Análisis

Fuente. Elaboración propia

Tabla 2. Software base

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

Fuente. Elaboración propia

Tabla 3. Respaldo de la información

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

Fuente. Elaboración propia

10.2 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 y sedes 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

10.2.1 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.

Tabla 4 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).

Fuente. Elaboración propia

Tabla 5 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.

Fuente. Elaboración propia

10.3 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.

10.3.1 Corte General del Fluido eléctrico

a. Si se presenta un cortocircuito, la UPS mantendrá activo los servidores, mientras se repara la falla eléctrica.

b. Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia).
c. 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.
d. 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).

10.3.2 Indisponibilidad Del Centro De Cómputo:

10.3.2.1 Destrucción del centro de cómputo

a. Contar con el inventario total de sistemas actualizado.
b. Identificar recursos de hardware y software que se puedan rescatar.
c. Salvaguardar los Back Up de información realizada.
d. Identificar un nuevo espacio para restaurar el Centro de Cómputo.
e. Presupuestar la adquisición de software, hardware, materiales, personal y transporte.
f. Adquisición de recursos de software, hardware, materiales y contratación de personal.
g. Iniciar con la instalación y configuración del nuevo centro de cómputo.
h. Restablecer los Back Up realizados a los sistemas.

10.3.2.2 Perdida de servicio internet

a. Realizar pruebas para identificar posibles problemas dentro de la entidad.
b. Si se evidencia problema en el hardware, se procederá a cambiar el componente.
c. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor.
d. Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
e. Si el daño es por parte del proveedor que suministra el servicio, se debe validar tiempo en restablecerse.
f. Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
g. Realizar pruebas de operatividad del servicio.
h. Servicio de internet activo.

10.3.2.3 Daño en Base de Datos

a. Verificar el daño ocurrido en la información.

b. Se restaura la Base de Datos con la copia a corte de ocurrido el evento.
c. Verificar la información con los usuarios.

10.3.2.4 Capacidad de Almacenamiento en los Servidores:

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

10.4 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.

10.4.1 Incendio o Fuego

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

Tabla 6 Incendio o fuego

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 cuenta con un extintor debidamente cargado.	• Se cumple
• 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.

Fuente. Elaboración propia

10.4.2 Robo Común de Equipos y Archivos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Moderado

Tabla 7 Robo común de equipos

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.

Fuente. Elaboración propia

10.4.3 Falla en los Equipos

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Table 8 falla en equipos

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)

Fuente. Elaboración propia

10.4.4 Acción de Virus Informático

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Continuo

Grado de Impacto: Grave

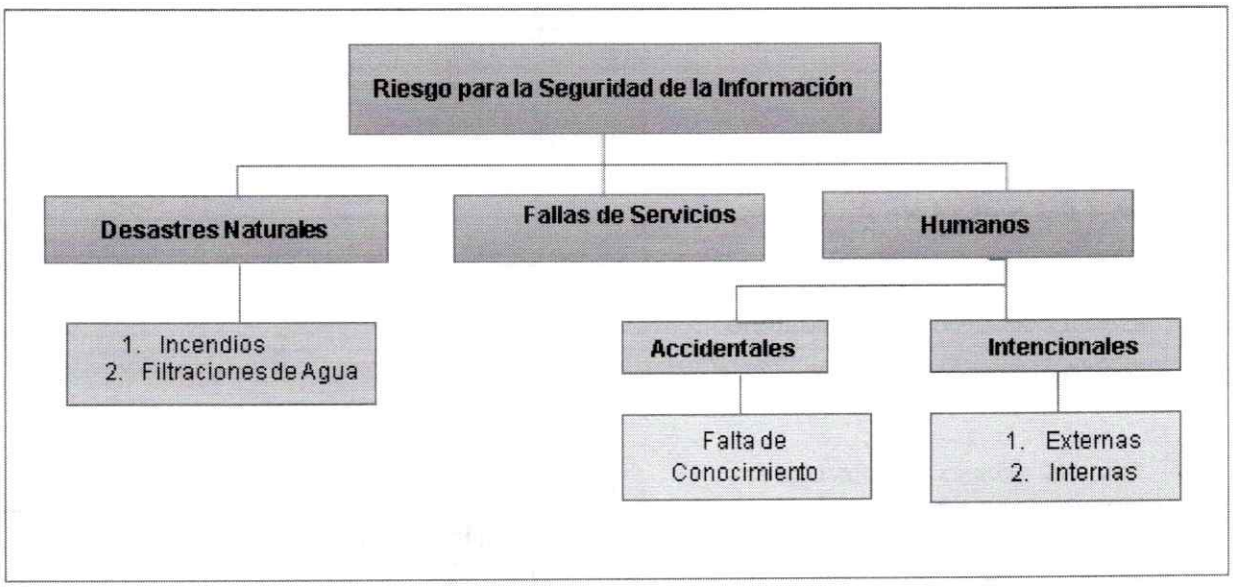
Tabla 9 acción de virus informático

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

Fuente. Elaboración propia

10.4.5 Riesgos para la seguridad de la información

Imagen 1 riesgos seguridad de la información



Fuente. Elaboración propia

10.4.5.1 Riesgos Por Naturaleza Física

Tabla 10 riesgo 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

Fuente. Elaboración propia

10.4.5.2 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.

Tabla 11 riesgos ambientales

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

Fuente. Elaboración propia

10.4.6 Accesos No Autorizados

Grado de Negatividad: Grave

Frecuencia de Evento: Aleatorio

Grado de Impacto: Grave

Tabla 12 acceso no autorizados

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.
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.

Fuente. Elaboración propia

10.5 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.

10.5.1 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).

10.6 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:

Tabla 13 documentos contingencia

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

Fuente. Elaboración propia

10.6.1 Tiempos para activación de la contingencia:

- Consulta externa y servicio de urgencias: Se activará la contingencia en estos servicios transcurridos 45 minutos de falla en el sistema (SAHI).
- Servicios hospitalarios: Se activará la contingencia transcurridos 45 minutos de falla en el sistema (SAHI).

Nota: En el caso de presentarse una emergencia clínica el plan de contingencia se activará de forma inmediata y será informado a todo el equipo asistencial y administrativo.

10.*6.1.1 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.

10.6.1.2 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.

10.6.1.3 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.

10.7 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.

10.8 Plan de actividades

Con el fin de hacer seguimiento y cumplir a cabalidad con lo establecido en el Plan de Gerencia de la Información 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

.

11. 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.

Los documentos que se maneja para hacer seguimiento son:

- Informe de Gestión
- Reuniones con los líderes de área y compromisos adquiridos.
- Seguimiento a las actividades que se encuentran relacionadas en el plan de gerencia de la información

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ing. Erwing Jesid Dávila G. **WEBMASTER**		
Juan Gabriel Rojas Gómez **Gestión Documental.**	Ing. Mario U. Bayona **Coordinador sistemas**	Natalia Sofía Ojeda Ortiz **Gerente**
FECHA: 14/01/2026	FECHA: 14/01/2026	FECHA: 14/01/2026

RESOLUCIÓN Nº 012
14 de enero de 2026

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN ANUAL DE CONTINGENCIA DE LA ESE HOSPITAL PSIQUIÁTRICO SAN CAMILO PARA LA VIGENCIA 2026"

La Gerente de la Empresa Social del Estado Hospital Psiquiátrico San Camilo, nombrada mediante Decreto 379 del 22 de marzo de 2024, expedido por el Gobernador de Santander y posesionada con Acta No. 017 del 01 de Abril de 2024, con efectos legales y fiscales, a partir del 01 de abril de 2024, en ejercicio de las atribuciones Constitucionales, legales, estatutarias y en especial las conferidas en el Acuerdo Nº 003 del 06 de febrero de 2006, y el Acuerdo N° 17 del 19 de diciembre de 2018, expedidos por la Junta Directiva de la Entidad, y

CONSIDERANDO:

Que la Empresa Social del Estado Hospital Psiquiátrico San Camilo, es una entidad prestadora de servicio de salud mental, descentralizada del orden departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa, de conformidad con lo dispuesto en el Decreto 0098 del 14 de agosto de 1995, *"Por medio del cual se transforma un Hospital Departamental en una Empresa Social del Estado"*, proferido por el Gobernador de Santander y el Acuerdo de Junta Directiva N° 003 de 2006, *"Por medio del cual se reforma el Estatuto de la Empresa Social del Estado Hospital Psiquiátrico San Camilo"*, expedido por la Junta Directiva de la Entidad.

Que de conformidad con el Manual Operativo del Modelo Integrado de Planeación y Gestión, MIPG, en la 5º Dimensión denominada "Información y Comunicación", define la comunicación como un elemento articulador con todos los procesos de la institución, para facilitar el ciclo de gestión y un flujo de información adecuado, y precisa contar con canales de comunicación acordes con las capacidades organizacionales y con lo previsto en la Ley de Transparencia y Acceso a la Información.

Que, en ese sentido, resulta indispensable que la información y los documentos que la soportan, ya sean escritos, electrónicos, audiovisuales u otros, sean gestionados de manera adecuada, con el fin de facilitar la operación institucional, el desarrollo de las funciones misionales, la seguridad y protección de los datos, así como la trazabilidad de la gestión.

Que el Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia, en su Grupo de Estándares de Gerencia de la Información, específicamente en el Estándar 143, Código: (GI2), requiere que exista un proceso para planificar la gestión de la información en la organización; este proceso está documentado, implementado y evaluado en un plan de gerencia de la información.

Que la Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, garantiza a los ciudadanos el acceso a la información pública y establece la obligación de las entidades de responder de buena fe, de manera adecuada, veraz, oportuna y gratuita a las solicitudes de información, promoviendo además la cultura de la integridad y el control social.

Que la ESE Hospital Psiquiátrico San Camilo para las vigencias 2026 – 2028, dentro de la ruta crítica para el desarrollo de la auditoría para el mejoramiento de la calidad de la atención en salud, ha establecido un Plan de Gerencia de la Información, elaborado e implementado por el grupo de Gerencia de la Información, orientado a garantizar la seguridad, continuidad, oportunidad y aseguramiento de la calidad de la gestión de la

información para todas las partes interesadas.

Que, así mismo, los documentos CONPES 3701 de 2011 y 3854 de 2016 establecen los lineamientos de la Política Nacional de Ciberseguridad, Ciberdefensa y Seguridad Digital, orientados a la protección de los activos de información del Estado.

Que la norma internacional ISO 22301:2019 es la última versión de la norma para sistemas de gestión de la continuidad de negocio (SGCN) proporciona un marco de buenas prácticas para ayudar a las organizaciones a gestionar eficazmente el impacto de una interrupción en su funcionamiento.

Que la guía técnica GTC-ISO/IEC 27031 colombiana del 2016, Tecnología de la información - Técnicas de seguridad, emite directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad de negocio.

Que la ISO 22317:2021 Seguridad y resiliencia – Sistemas de Gestión de Continuidad de Negocio – Directrices para el análisis de impacto empresarial (BIA) proporciona una serie de pautas a la empresa para implementar y mantener su BIA.

Que la Norma Técnica Colombiana NTC-ISO-IEC 27001 es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan.

Que los Lineamientos MINTIC LI.ST.05, LI.ST.09, LI.ST.10, LI.ST.13 del 2015, Orientaciones de carácter general que corresponden a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano, específicamente en operación y soporte de los servicios tecnológicos.

Que el Estándar 151, Código GI10, del Manual de Acreditación en Salud, dispone que debe existir un plan de contingencia diseñado, implementado y evaluado, que garantice el normal funcionamiento de los sistemas de información de la organización, manuales o automatizado, incluyendo mecanismos para prevenir eventos adversos relacionados con el manejo de los sistemas de información.

Que, en virtud de lo anterior, se hace necesario adoptar el Plan Anual de Contingencias para los Sistemas de Información de la Empresa Social del Estado Hospital Psiquiátrico San Camilo para la vigencia 2026.

En mérito de lo anterior,

RESUELVE:

ARTÍCULO PRIMERO: ADOPCIÓN: Adoptar el Plan de Contingencias para los Sistemas de Información del ESE Hospital Psiquiátrico San Camilo el cual para todos los efectos legales forma parte integral de la presente Resolución, para la Vigencia 2026.

ARTÍCULO SEGUNDO: ESTRUCTURA: El Plan de Contingencias para los Sistemas de Información para la vigencia fiscal 2026, está contenido en el Anexo Técnico No 001, el cual forma parte integral de la presente resolución en veintiún (21) folios útiles. Por tanto, en dicho anexo se enuncian las actividades propuestas para su cumplimiento.

ARTÍCULO TERCERO: SEGUIMIENTO Y EVALUACIÓN: Corresponde a cada referente de proceso, rendir información del grado de avance de ejecución de las actividades bajo su responsabilidad, de manera trimestral, siendo los líderes de cada área de la gerencia de la información, los responsables para realizar esta actividad.

ARTÍCULO CUARTO: ÁMBITO DE APLICACIÓN: El presente Plan de Contingencias para los Sistemas de Información, es de obligatorio cumplimiento para todos los funcionarios, contratistas, colaboradores y personal vinculado a la Empresa Social del Estado Hospital Psiquiátrico San Camilo, en cualquier nivel y en todas las áreas de la misma.

ARTÍCULO QUINTO: DIVULGACIÓN: El Plan de Contingencias para los Sistemas de Información se divulgará a los miembros de la ESE y a sus grupos de interés por los funcionarios competentes.

ARTÍCULO SEXTO: REFORMAS: El Plan de Contingencias para los Sistemas de Información podrá ser reformado por decisión del Gerente, adaptándose a las necesidades de la Entidad y a la normatividad vigente. El Gerente informará a los grupos de interés de la ESE, los cambios introducidos.

ARTÍCULO SÉPTIMO: VIGENCIA: La presente resolución rige a partir de la fecha de su expedición y deja sin efectos todos los actos administrativos que le sean contrarios.

Se expide en Bucaramanga, a los 14 días del mes de Enero de dos mil veinticinco 2026.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

NATALIA SOFIA OJEDA ORTIZ
Gerente

Revisó Aspectos Jurídicos: Mayra Alejandra Téllez Romero
Jefe Oficina Asesora Jurídica

Proyectó: Erwing Jesid Dávila G.
WebMaster Institucional

Revisó Aspectos Técnicos: Mario J. Bayona
Proceso Administrativo Gestión de la Información.