PROCEDIMIENTO PLAN DE CONTINGENCIA INFORMÁTICO

EJES TEMÁTICOS DE ACREDITACIÓN

GESTIÓN DEL RIESGO	***MEJORAMIENTO CONTINUO***
	

SANTIAGO DE CALI, SEPTIEMBRE 2021

CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
2.1. PRINCIPALES MÓDULOS DEL SISTEMA PANACEA IDENTIFICADOS:... 4
2.2. RESPALDO DE LA INFORMACIÓN 5
2.3. ACTIVOS SUSCEPTIBLES DE DAÑO 5
3. NORMATIVA 6
4. DEFINICIONES 6
5. RIESGOS 8
6. CONTENIDO 8
6.1. ACTIVIDADES A REALIZAR DE MANERA GENERAL 8
6.2. FALLA DE CONTINUIDAD DEL FLUIDO ELÉCTRICO 9
6.3. INCENDIO O FUEGO 9
6.4. ROBO COMÚN DE EQUIPOS Y ARCHIVOS 10
6.5. FALLA POR ATAQUE MASIVO DE VIRUS INFORMÁTICO 11
6.6. FALLA EN LOS EQUIPOS 11
6.7. MANEJO ERRADO DEL SISTEMA DE INFORMACIÓN / ACCESOS NO AUTORIZADOS 12
6.8. FENÓMENOS NATURALES 12
6.9. FALLA DEL SISTEMA DE INFORMACIÓN PANACEA 13
6.10. FALLA DEL SERVICIO DE INTERNET 13
6.11. FALLA DEL SERVICIO DE INTRANET 14
6.12. FALLA DEL SERVIDOR 14
6.13. RECUPERACIÓN DE INFORMACIÓN DEL SISTEMA DE INFORMACIÓN PANACEA 14
6.14. AUSENCIA DEL PERSONAL DE SISTEMAS 15
6.15. RECURSOS DE CONTINGENCIA 16
6.16. ACTIVIDADES A REALIZAR POR ÁREA 16
6.16.1. Facturación 16
6.16.2. Admisiones urgencias 16
6.16.3. Anexos y autorizaciones 17
6.16.4. Asignación de citas 17
6.16.5. Consulta externa 17

6.16.6. Manejo de atención por historia clínica (incluye ingreso de: urgencias, hospitalización, salas de cirugía y odontología) 18

6.16.7. Enfermería 18

6.16.8. Apoyo diagnóstico (laboratorio clínico e imagenología) 19

6.16.10. Referencia y contrareferencia 20

7. INDICADORES 20

8. ANEXOS 20

9. CONTROL DE REGISTROS 22

10. ELABORO, REVISO Y APROBÓ 22

1. OBJETIVO

GENERAL

Definir las actividades de planeación, preparación y ejecución de acciones destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fallas técnicas o humanos en la institución.

ESPECÍFICOS

- Generar acciones que garanticen el funcionamiento de la tecnología informática y la recuperación en el menor tiempo posible de cualquier falla que interrumpa el servicio.
- Mantener la conectividad, acceso a internet, como también los desarrollos propios y aplicaciones del hospital.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y/o infraestructura informática. Proteger la propiedad de la ESE y otros activos.
- Proteger al sistema de información de pérdidas irreparables de información procesada.

2. ALCANCE

Es necesario la identificación previa de cuáles de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

2.1. PRINCIPALES MÓDULOS DEL SISTEMA PANACEA IDENTIFICADOS:

Área administrativa

- Nomina
- Cartera
- Presupuesto
- Tesorería, caja
- Activos fijos
- Contabilidad, cuentas por pagar y por cobrar
- Inventarios
- Facturación
- Citas

- Admisiones y autorizaciones
- Referencia y contrareferencia

Área asistencial

- Historia Clínica
- Urgencias
- Triage
- Consulta especializada
- Laboratorio Clínico
- Observación e internación
- Odontología
- Procedimientos
- Terapias física y respiratoria
- Cirugía
- Imágenes diagnósticas
- Unidad de cuidados intensivos
- Homecare

2.2. RESPALDO DE LA INFORMACIÓN

- Backup de la Base de Datos PANACEA
- Copia de seguridad en la nube
- Discos duros externos
- Unidad NAS

2.3. ACTIVOS SUSCEPTIBLES DE DAÑO

- Personal
- Hardware
- Documentación
- Software y utilitarios
- Datos e información
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

3. NORMATIVA

ISO 27001: (Organización Internacional de Estandarización) define el riesgo informático como: “La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños.”

Ley 594 de 2000: Ley General de Archivos; Establece las reglas y principios que regulan la función archivistas del estado.

Ley 734 de 2000: Por la cual se expide el Código Disciplinario Único.

> Artículo 34 Numeral 22: “Son deberes de todo servidor público: Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.”
>
> Artículo 34 Numeral 28. Establece: “Son deberes de todo servidor público: Controlar el cumplimiento de las finalidades, objetivos, políticas y programas que deban ser observados por los particulares cuando se les atribuyan funciones públicas.
>
> Artículo 35 Numeral 9: “A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres.
>
> Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.

Ley 527 de 1999: Que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

4. 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.

Contingencia: 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.

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.

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).

Plan de Contingencia: Son procedimientos que definen como una entidad continuará 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: 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. Existen distintos tipos de riesgo:

- **Riesgos Naturales:** Tales como mal tiempo, terremotos, etc.
- **Riesgos Tecnológicos:** Tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
- **Riesgos Sociales:** como actos terroristas y desórdenes.

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.

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).

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.

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.

5. RIESGOS

RIESGOS	ACCIONES
Incendio o Fuego	Tener el extintor indicado en las zonas cercanas a la ubicación de los equipos, es decir extintor tipo c, así mismo garantizar capacitación al personal de la institución en el manejo del mismo.
Acción de virus informático	Evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.
Fenómenos naturales	Tener señalados e identificados los puntos de encuentro frente a emergencias naturales
Robo común de equipos y archivos	Tener todos los equipos registrados en el inventario de activos de la institución, así mismo deben estar correctamente identificados con su sello de identificación institucional, y garantizar que el personal de vigilancia tenga conocimiento de esta identificación al momento de registra el ingreso y egreso de equipos a la institución.
Accesos no autorizados	Realizar la creación del usuario en el sistema de información en el cual se deben dar los permisos según el perfil y el rol de cada usuario que necesite para sus actividades diarias. Restringir el acceso al personal que no corresponda al área de sistemas.
Fallo en equipos	Identificar la causa de la falla, realizar un plan de acción como revisión periódica y mantenimiento preventivo.
Ausencia del personal de sistemas	Diseñar un plan estratégico donde se garantice por lo menos la presencia de una persona del área de sistemas

6. CONTENIDO

6.1. ACTIVIDADES PARA REALIZAR DE MANERA GENERAL

Ante situaciones anormales que ocasionen alguna de las fallas antes mencionadas, se procederá según corresponda.

6.2. FALLA DE CONTINUIDAD DEL FLUIDO ELÉCTRICO

La institución cuenta con planta eléctrica cuya responsabilidad recae sobre el área de mantenimiento, y estará encargada de brindar energía eléctrica a las diferentes áreas del hospital. Igualmente, el área de sistemas cuenta con 50 KVA en UPS la cuales soportan los servidores institucionales y equipos de Cómputo y comunicaciones.

Situación	Acción
Falla de continuidad del fluido eléctrico	1. Revisar la carga de la UPS (la carga dura alrededor de 40 minutos) y determinar el tiempo restante de suministro eléctrico auxiliar (indefinido ya que depende de la disponibilidad del combustible y el recurso humano de mantenimiento disponible en la contingencia). 2. Llamar a gestión de tecnología y mantenimiento para identificar si la falla es de la red pública eléctrica o se debe a un daño local. 3. Por seguridad se deben apagar los equipos conectados a la UPS. 4. En caso de falla general se deberá esperar a que ésta se normalice, para de nuevo encender los equipos. 5. Si la falla es originada por algún factor local, se deberá revisar el tablero de breakers e inspeccionar si algún corto circuito se presentó por algún equipo de cómputo u otra causa como elementos que demanden alto consumo de energía eléctrica como estufas, neveras, etc. Se deberá solicitar el apoyo de gestión de tecnología y mantenimiento para que el electricista revise los circuitos conectados a la UPS. 6. Una vez gestión de tecnología y mantenimiento localice la falla local, se procede a la reparación o reemplazo de los componentes que causaron la falla y proceder a restablecer el suministro eléctrico y no encender los equipos de cómputo hasta después de 10 minutos restablecido el servicio. 7. Si hay interrupción de energía se sostendrán con los UPS mientras que la planta empieza a funcionar.

6.3. INCENDIO O FUEGO

La institución cuenta con sistemas de protección, contra incendios, como son, extintores manuales, equipos de bajo consumo, vías de acceso y de evacuación, amplias, etc., sin embargo, algún incidente involuntario, puede ocasionar, el inicio de un Incendio.

Situación	Acción

Incendio o fuego	1. Al detectar el inicio del incendio se procede a dar la alarma a todo el personal del área, áreas cercanas y a los bomberos. 2. Desconectar las fuentes de alimentación eléctricas (sin riesgo de exponer la vida). 3. Si el tiempo lo permite y si la fuente del siniestro está lejos, pero se puede propagar hacia los equipos principales de cómputo (servidores) deberá retirar los equipos hacia un lugar seguro, discos o últimas copias que tenga a la mano. 4. Se deberá sofocar el fuego utilizando el extintor correcto para el tipo de fuego generado (extintor tipo c). 5. Se debe tener en cuenta que estas acciones se realizan si y solo si, no signifiquen riesgo de exponer la vida del personal, en caso contrario alejarse del sitio y esperar a las unidades de emergencias.

6.4. ROBO COMÚN DE EQUIPOS Y ARCHIVOS

Situación	Acción
Robo común de equipos y archivos	1. Ingreso solo del personal autorizado (personal del área de sistemas de información, vigilancia y autoridades competentes como policía nacional en caso de robo) a las áreas restringidas donde se encuentra la Sala de Servidores y/o otros lugares donde se encuentren los equipos informáticos; si otras personas ingresan debe ser con autorización y coordinación de la jefatura inmediata y en los tiempos establecidos y/o coordinados. 2. Vigilancia con cámaras de seguridad en las áreas consideradas clave y en caso que no se encuentre personal en una de esas áreas deberá estar cerrado por motivos de seguridad. 3. La dependencia en donde se encuentre el servidor no debe ser accesible para nadie, excepto para el administrador de la red y/o la persona responsable del mismo. 4. Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves o bloqueos de las PC. 5. Solicitar clave de ingreso a la red y a los sistemas que están en red. 6. Solicitar orden y/o autorización de retiro o ingreso de equipos a la institución.

	7. Existe en las salidas de la institución formato de ingresos y salidas de equipos GALH-F-017-33 que tiene que firmar cada vez que salga o ingrese un equipo de la institución o de tercero.

6.5. FALLA POR ATAQUE MASIVO DE VIRUS INFORMÁTICO

Situación	Acción
Falla por ataque masivo de virus informático.	1. Identificar con antivirus actualizados que tipo de virus es el que se está propagando. 2. Según lo registrado en la página web de los antivirus seguir las recomendaciones de seguridad, incluyendo parches de los sistemas operativos. 3. Aislar de la red los equipos infectados, hasta definir una manera eficaz de erradicar el virus y detectar su medio de propagación. 4. Elaborar guía rápida paso a paso de eliminación del virus, y aplicarla en los equipos aislados y desinfectar. 5. Estos archivos (exe, com, etc.) serán reemplazados del disco original de instalación o del backup. 6. Parchar los equipos vulnerables a ese tipo de infección para evitar propagación. 7. Los equipos que se encuentran aislados luego de ser vacunados, se conectan uno a uno a la red y monitorean su comportamiento. El encargado de este proceso será el coordinador del área de sistemas, en caso de que él no pueda realizar esta acción, designara a alguien del personal del área de sistemas de información.

6.6. FALLA EN LOS EQUIPOS

Situación	Acción
Falla en los equipos	Para disminuir el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo y correctivo a los equipos de cómputo e implementar acciones de limpieza continua de las partes que componen un equipo de cómputo; Se debe tener registro del mantenimiento realizado a los mismo, de igual manera un inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

	El área donde se encuentran los servidores debe estar con la ventilación necesaria, con la seguridad e instalación correcta de las redes eléctricas, el orden y limpieza de la infraestructura tecnológica que puede afectar a los servidores o disminuir su tiempo de vida. También se pueden generar por problemas eléctricos y bajones de energía, por lo cual el personal de gestión de tecnología y mantenimiento debe realizar revisiones al contador central y finiquitar este problema.

6.7. MANEJO ERRADO DEL SISTEMA DE INFORMACIÓN / ACCESOS NO AUTORIZADOS

Situación	Acción
Manejo errado del Sistema de información/ accesos no autorizados	1. Cuando hay manejo del sistema errado, la persona que identifique esta inconsistencia llama al soporte del área de sistemas por las áreas de servicio para su revisión y arreglo si es el caso, si no se informara de igual manera al coordinador del área de sistemas para que se comuniquen con la empresa proveedora del software PANACEA. 2. Se realizan continuamente inducción y retroalimentación del sistema de información PANACEA al personal que labora en la institución y tiene acceso al sistema de información por las actividades que realiza. 3. Todos los usuarios del sistema de información PANACEA manejan su usuario y su clave respectivamente que son asignadas por el área de sistemas, cuando el personal se retira y se va de vacaciones es informado a sistemas para su inactivación. 4. Existe un Rol de administrador del sistema que hace las funciones.

6.8. FENÓMENOS NATURALES

Situación	Acción
Tormentas eléctricas	Cuando hay tormentas eléctricas se trata de que el personal apague los equipos y espere a que pase el evento para evitar daños de la información.

En caso de daño en el fluido eléctrico se procede a esperar que la planta se encienda, el servidor o el área de sistemas cuenta con una malla a tierra que los protege.

6.9. FALLA DEL SISTEMA DE INFORMACIÓN PANACEA

Situación	Acción
Falla del sistema de información PANACEA	1. El personal de sistemas de información que este de turno deberá verificar que el servidor se encuentre en servicio y con funcionamiento normal, en caso de encontrarse bloqueado reiniciar manualmente el servidor, una vez termine el proceso de cargue, verificar que la aplicación PANACEA funcione correctamente ingresando a este sistema. 2. En caso de que el servidor se encuentre trabajando normalmente, el personal de sistemas de información deberá verificar que el servicio de SQL esté activo, en caso contrario reiniciar el servicio verificando la conexión con la base de datos de PANACEA. 3. Si el origen de la falla no corresponde a los casos anteriores, el personal de sistemas de información que haya detectado la fallada deberá llamar a CNT SISTEMAS DE INFORMACION SAS al teléfono de soporte y reportar la anomalía vía correo electrónico **(ver anexo 1, punto 1).** 4. Una vez superada solicitar informe de causas.

6.10. FALLA DEL SERVICIO DE INTERNET

Situación	Acción
Falla del servicio de internet	1. El personal de sistemas de información que este de turno deberá verificar que el router cisco se encuentre encendido, en caso contrario ajustar el suministro eléctrico. 2. El personal de sistemas de información que este de turno deberá realizar ping desde un equipo conectado a la red de datos institucional a la dirección IP 10.10.1.2, en caso de no recibir respuesta verificar la conexión LAN, si es correcta se deberá reiniciar manualmente el router desconectado el suministro eléctrico. 3. En caso de que haya respuesta del ping, el personal de sistemas de información que haya detectado la falla, deberá verificar el servicio de internet con los proveedores CLARO y EMCALI a las líneas de soporte **(ver anexo 1, punto 2).**

6.11. FALLA DEL SERVICIO DE INTRANET

Situación	Acción
Falla del servicio de intranet	1. El personal de sistemas de información que este de turno deberá verificar el correcto funcionamiento del servidor de nombre SERVER1. 2. El personal de sistemas de información que este de turno deberá verificar el servicio de la aplicación WAS, en caso de estar detenido se sugiere reiniciar el servidor. 3. El personal de sistemas de información que este de turno deberá verificar la conexión de red del SERVER1 con dirección IP 10.10.1.2 o 172.16.4.200

6.12. FALLA DEL SERVIDOR

La institución cuenta con 2 servidores (2 de Aplicaciones locales, 1 aplicación IP pública, 1 de base de datos), el primero cuenta con discos y fuentes redundantes, en caso de que cualquiera de los servidores falle por algún elemento de hardware, se deberá recurrir al equipo marca DELL POWEREDGE M620 y HP.

Situación	Acción
Falla del servidor	1. El equipo HP tiene preinstalado SQL y demás aplicaciones necesarias para el determinado momento cargar las copias de seguridad de alguno de los servidores. 2. los equipos DELL tienen preinstalado el servicio de aplicaciones. 3. Restaurar la última copia de seguridad externa para activar su funcionamiento.

6.13. RECUPERACIÓN DE INFORMACIÓN DEL SISTEMA DE INFORMACIÓN PANACEA

Situación	Acción
Recuperación de información del sistema de información PANACEA	Al sistema de información PANACEA se le realiza una copia diaria de seguridad, que en primera instancia se copia en la unidad D del servidor de aplicaciones, luego es copiada al equipo del denominado técnico 1 y luego se deposita en el NAS y posteriormente al DRIVE en la nube. Esta recuperación de información del aplicativo PANACEA solo se realizará de las

	copias de seguridad en caso de ser imposible recuperar la base de datos del servidor. Se debe solicitar el acompañamiento de la empresa PANACEA. Para realizar esta labor, llamando al teléfono de soporte y reportar la anomalía vía skype o al correo electrónico **(ver anexo 1, punto 3).**

6.14. AUSENCIA DEL PERSONAL DE SISTEMAS

Situación	Acción
Ausencia del personal de sistemas	1. Se cuenta con el personal suficiente, totalmente capacitado y con alta experiencia en hardware, software y redes para dar apoyo en la institución, en su jornada laboral deberán estar atentos al llamado. 2. El soporte técnico de lunes a viernes de 7am a 6pm, sábados de 9am a 2pm, domingos y festivos por disponibilidad, en caso de haber contingencia presencia inmediata del personal del área.

En caso de tal de que haya pérdida total o destrucción del centro de cómputo es indispensable que el área:

- Evalué los daños, y se atenderá como prioridad los procesos misionales, la facturación y el registro de la historia clínica habilitando el servidor de contingencia.
- Realizar inventario de equipos de cómputo.
- Identificar recursos de hardware y software que se puedan rescatar.
- Salvaguardar los backup de información.
- Gestione la recuperación y puesta en marcha de los equipos, compra de equipos dañados.
- Cree equipos de trabajo, asignando actividades a las personas que conocen de sistemas del hospital, y cada uno contará con un líder para mirar el avance de los trabajos.
- Busque un nuevo espacio para el centro de cómputo.
- Presupuestar compra de hardware, software, materiales y contratación de personal.
- Iniciar con la instalación del nuevo centro de cómputo.
- Restablecer los backup realizados anteriormente.
- Se debe verificar continuamente que lo realizado se encuentre funcionando correctamente.

6.15. RECURSOS DE CONTINGENCIA

- Debe existir una reserva de ups, monitores, teclados, mouse, cartuchos, impresoras etc. Para no parar el servicio en almacén se encuentran o si no se reemplazan por otros sistemas.
- Se realiza backup diario de la información.
- Manual de los funcionarios de sistemas.
- Inventario de todos los equipos de cómputo.
- Diagrama lógico de toda la red.
- Todos los equipos de cómputo deben estar protegidos con unos ups para evitar daños en su fuente de poder y demás hardware.
- Puede haber un daño físico en el servidor por daño de disco duro, pero se tiene respaldo de otro servidor alterno.
- Cuando hay un daño en el sistema, Gestión de sistemas avisa al almacén para que este entregue a las áreas de servicio la papelería necesaria para prestar los servicios.
- Se tiene en los computadores de los diferentes servicios y jefes de procesos (formatos necesarios para historia clínica y demás).
- Se cuenta con soporte de los ingenieros de PANACEA, vía telefónica y una cuenta de Skype directa **(ver anexo 1, punto 4).**

6.16. ACTIVIDADES A REALIZAR POR ÁREA

Se priorizan las áreas que garanticen la atención del usuario, es decir los módulos más afectados en caso de presentar algún evento que impide garantizar el funcionamiento de los procesos esenciales para la atención del paciente.

6.16.1. Facturación

- Una vez se restablezca el sistema, el facturador debe dirigirse a archivo historia clínica para solicitar los documentos del paciente para completar la factura

6.16.2. Admisiones urgencias

- Se diligencian los datos necesarios para la correcta identificación del usuario en el formato COME-F-018-01. Una vez restablecido el servicio se realizará el ingreso al sistema de información PANACEA de la persona, actividad que realiza el personal del área de admisiones que este de turno en el momento.
- La validación de derechos se realizará por medio telefónico, base de datos, páginas de las EAPB, ADRES o SISBEN, según corresponda.

- Se realiza anexo 2 en formato establecido (Excel o Word) con los datos que haya diligenciado el medio, cumpliendo con los tiempos de reporte establecidos en el decreto 4747 de 2007 y en la resolución 3047 de 2008.

Legalización para consulta externa

- En caso de falla en el suministro de internet se verifica que la autorización este vigente y se direcciona al paciente al consultorio correspondiente.

6.16.3. Anexos y autorizaciones

- Se realiza anexo 3 en formato establecido (Excel o Word), cumpliendo con los tiempos de reporte establecidos en el decreto 4747 de 2007 y en la resolución 3047 de 2008.
- Una vez restablecido el internet se realizan los cargues en plataforma o envíos según corresponda la EPS.

6.16.4. Asignación de citas

- Al fallar el sistema de información PANACEA, se debe tener la referencia del día que no se haya iniciado con la generación de cupos por especialidad, el personal encargado tomará información básica para la asignación de citas como lo son:
    - número de identificación
    - nombre completo.
    - número de teléfono de contacto (por lo menos dos números de contacto).
    - correo electrónico.
    - nombre de la EPS.
    - número de autorización.
    - El paciente presencial se le solicita la información anterior más una copia de la autorización

Al momento que se restablezca el sistema PANACEA, con previa validación de derechos se asignará la cita y se informará por vía telefónica y correo electrónico.

6.16.5. Consulta externa

Garantizar la atención al paciente de manera continua, oportuna y eficiente es el objetivo por lo cual se estandarizaron formatos que lo permitan (Ver anexos 13, 18, 26-29).

- Si el equipo de cómputo no presenta daños, se podrá hacer uso de herramientas office para realizar el registro de la atención prestada al paciente en los formatos entregados en medio magnético por el proceso de calidad y/o jefe del proceso
- Si el daño es total en el manejo del equipo informático se procederá a realizar el registro de forma manual, la cual será entregada a archivo de historia clínica con la relación de los documentos y diagnóstico de la atención, quienes escanean el documento y lo anexan a la historia clínica en el sistema de información PANACEA, esto incluye, historia clínica, epicrisis, órdenes médicas y demás que sean necesarias.

6.16.6. Manejo de atención por historia clínica (incluye ingreso de: urgencias, hospitalización, salas de cirugía y odontología)

Garantizar la atención al paciente de manera continua, oportuna y eficiente es el objetivo por lo cual se estandarizaron formatos que lo permitan (Ver anexos 3- 20).

- Si el equipo de cómputo no presenta daños, se podrá hacer uso de herramientas office para realizar el registro de la atención prestada al paciente en los formatos entregados en medio magnético por el proceso de calidad y/o jefe del proceso, esto incluye, historia clínica, epicrisis, órdenes médicas y demás que sean necesarias.
- Si el daño es total en el manejo del equipo informático se procederá a realizar la historia clínica de forma manual, la cual será entregada a archivo de historia clínica con la relación de los documentos y diagnóstico de la atención, quienes escanean el documento y lo anexan a la historia clínica en el sistema de información PANACEA, esto incluye, historia clínica, epicrisis, órdenes médicas y demás que sean necesarias.
- Archivo de historia clínica debe entregar al proceso de facturación una copia de las atenciones para ser cruzadas en el manejo de los RIPS.

6.16.7. Enfermería

Garantizar la atención al paciente de manera continua, oportuna y eficiente es el objetivo por lo cual se estandarizaron formatos que lo permitan (Ver anexos 3- 20).

- Si el equipo de cómputo no presenta daños, se podrá hacer uso de herramientas office para realizar el registro de la atención prestada al paciente en los formatos entregados en medio magnético por el proceso de calidad y/o Jefe del proceso, esto incluye notas de enfermería, administración de medicamentos, notas de procedimientos realizados y demás que sean necesarios.
- Si el daño es total en el manejo del equipo informático se procederá a realizar la historia clínica de forma manual, la cual serán entregada a archivo de

historia clínica con la relación de los documentos y diagnóstico de la atención, quienes escanean los documentos y lo anexan a la historia clínica en el sistema de información PANACEA, esto incluye notas de enfermería, administración de medicamentos, notas de procedimientos realizados y demás que sean necesarios.

- Archivo de historia clínica debe entregar al proceso de facturación una copia de los registros de atenciones para poder realizar factura de venta y presentación de los RIPS.

6.16.8. Apoyo diagnóstico (laboratorio clínico e imagenología)

Estos procesos por ser de apoyo diagnóstico, pueden ser resueltos de la siguiente manera:

Laboratorio clínico:

- Se realiza la toma de muestras según la orden médica generada.
- Se entrega al laboratorio clínico la muestra tomada con su orden médica.
- En caso de que la falla que se esté presentando afecte el sistema de información laboratorio externo, los resultados se generarán de forma manual para su posterior cargue al sistema y se entrega el resultado a enfermería utilizando los formatos establecidos en el plan de contingencia laboratorio HDMCR AYUD-M-014-14, para su ingreso a la carpeta de historia clínica y posterior análisis por parte del profesional a cargo del paciente.

Imagenología

- Se procede a llevar al paciente al área de imagenología solicitada (tomografía, ultrasonografías o rayos x) para la toma de la imagen que solicite el profesional y este mismo será devuelto para la atención.
- En caso de que la falla que presente, afecte el sistema de información de imagenología, las lecturas de la imagen se generarán de forma manual para su posterior cargue al sistema y se entrega el documento a enfermería, para su ingreso a la carpeta de historia clínica y posterior análisis por parte del profesional a cargo del paciente.

6.16.9. Farmacia

- Si el equipo de cómputo no presenta daños, se podrá hacer lo descrito en el procedimiento de dispensación y distribución de medicamentos y dispositivos médicos FARM-P-019-08.
- Si el daño es total en el manejo del equipo informático se procederá a realizar el registro de forma manual, y estos serán ingresados al sistema cuando se habilite.

- Se debe entregar a facturación consolidación de gastos de medicamentos e insumos por paciente.

6.16.10. Referencia y contrareferencia

Garantizar la atención al paciente de manera continua, oportuna y eficiente es el objetivo por lo cual en caso de contingencia se recurrirá a:

- Si las fallas son con el sistema de información PANACEA, y los soportes de la historia clínica son elaborados en los formatos (Excel o Word) se enviarán según corresponda.
- Debe existir formato de anexo 9 según resolución 3047 de 2008 y formatos de referencia y contrareferencia creados en herramientas office (ver anexos 22-24).
- Si el caso es fallas en el servicio de internet se comentarán los usuarios vía telefónica.
- Si la falla es en el servicio de telefonía se enviarán los documentos necesarios vía correo electrónico.

7. INDICADORES

NOMBRE DEL INDICADOR	FORUMULA
Indisponibilidad	$\frac{Total\ de\ horas\ de\ indisponibilidad\ del\ sistema\ integrado\ de\ informacion}{Total\ de\ horas\ disponibles\ en\ el\ mes} * 100$
Ejecución de plan de mantenimiento sistema de información	$\frac{Numero\ de\ mantenimientos\ ejecutados}{Numero\ total\ de\ mantenimientos\ preventivos\ programados\ en\ la\ vigencia} * 100$
Oportunidad de Requerimientos (Soporte técnico)	$\frac{Sumatoria\ total\ de\ los\ minutos\ de\ espera\ entre\ la\ solicitud\ y\ la\ respues\ y\ solucion}{Numero\ de\ solicitudes\ del\ periodo}$

8. ANEXOS

Anexo 1. Listado de números en caso de fallas.

Anexo 2. GALH-F-017-33 V1 Formato de ingreso y salida de equipos de cómputo.

Anexo 3. HOSP-F-004-71 V3 Solicitud de dietas

Anexo 4. HOSP-F-004-97 V2 Listado de pacientes de cada servicio a guardas de seguridad

Anexo 5. HOSP-F-004-70 V3 Autorización de ingreso de alimentos

Anexo 6. URGE-F-005-11 V2 Solicitud de insumos área asistencial

Anexo 7. HOSP-F-004-17 V3 Notas de enfermería

Anexo 8. HOSP-F-004-27 V3 Registro de glucometrías

Anexo 9. HOSP-F-004-29 V3 Registro de curaciones

Anexo 10. HOSP-F-004-13 V3 Registro de signos vitales

Anexo 11. HOSP-F-004-28 V3 Control diario de medicamentos

Anexo 12. URGE-F-005-15 V3 Control de suministro de oxigeno

Anexo 13. AMBU-F-003-04 V3 Solicitud de ayudas diagnosticas laboratorio

Anexo 14. HOSP-F-004-14 V3 Ordenes medicas

Anexo 15. HOSP-F-004-64 V3 Ordenes de salida

Anexo 16. URGE-F-005-07 V4 Historia clínica servicio de urgencias

Anexo 17. HOSP-F-004-15 V3 Evolución medica

Anexo 18. HOSP-F-004-30 V3 Solicitud de interconsulta

Anexo 19. HOSP-F-004-52 V1 Motivo para realizar remisión

Anexo 20. URGE-F-005-09 V3 Epicrisis resumen de historia clínica

Anexo 21. FARM-P-019-08 V3 Procedimiento de dispensación y distribución de medicamentos y dispositivos médicos.

Anexo 22. RECO-F-021-04 V1 Acta de apertura de medicamentos de la ambulancia medicalizada

Anexo 23. RECO-F-021-05 V2 Formato para el control de medicamentos e insumos de ambulancia medicalizada

Anexo 24. RECO-F-021-09 Formato de traslado en ambulancia (Historia clínica)

Anexo 25. AYUD-M-014-14 Plan de contingencia laboratorio HDMCR

Anexo 26. AMBU-F-003-65 Formula medica

Anexo 27. AMBU-F-003-19 Consulta externa

Anexo 28. CIRU-F-013-16 Solicitud de turno para operación y anestesia

Anexo 29. AYUD-F-014-07 Solicitud de cultivos

9. CONTROL DE REGISTROS

Versión	Fecha	Modificación o Cambio
1	Agosto 2013	Elaborado por primera vez
2	Septiembre 2021	Se realizan ajustes al contenido y alcance, se agregan los ítems de normativa e indicadores, se cambia el código de SINF-G-011-01 a SINF-P-011-02

10. ELABORO, REVISO Y APROBÓ

Elaborado por:	Revisado por:	Aprobado por:
CARLOS SALGADO Auxiliar de Enfermería	**GILBERTO IZQUIERDO RUIZ** Subdirector Administrativo	
LISETH MUELA Auxiliar Administrativa	**MARIO GONZALEZ HERNANDEZ** Jefe De Gestión De Sistemas De Información	**JUAN CARLOS MARTÍNEZ GUTIÉRREZ** Gerente

9. CONTROL DE REGISTROS

Versión	Fecha	Modificación o Cambio
1	Agosto 2013	Elaborado por primera vez
2	Septiembre 2021	Se realizan ajustes al contenido y alcance, se agregan los ítems de normativa e indicadores, se cambia el código de SINF-G-011-01 a SINF-P-011-02

10. ELABORO, REVISO Y APROBÓ

Elaborado por:	Revisado por:	Aprobado por:
CARLOS SALGADO Auxiliar de Enfermería	GILBERTO IZQUIERDO RUIZ Subdirector Administrativo	
LISETH MUELA Auxiliar Administrativa	MARIO GONZALEZ HERNANDEZ Jefe De Gestión De Sistemas De Información	JUAN CARLOS MARTÍNEZ GUTIÉRREZ Gerente

ANEXO 1. Listado de números en caso de fallas.

1. En caso de falla del sistema de información PANACEA	
Numero	**Correo**
3137351278	paulocesar268@gmail.com.

2. Falla del servicio de internet	
Numero de CLARO	**Numero de EMCALI**
324880456	3700000

3. Recuperación de información del sistema de información PANACEA		
Numero	**skype**	**Correo**
3137351278	william_albornoz@cnt.com.co	cristhian_acero@cnt.com.co

4. Soporte de ingenieros PANACEA			
Nombre	**Numero**	**skype**	**Correo**
Paulo Cesar ingeniero del área de sistemas	3137351278		paulocesar268@gmail.com
William Camilo albornoz soporte CNT		william_albornoz@cnt.com.co	
Soporte financiero Julieth Torres implementadora CNT	3102980851		