PLAN DE CONTINGENCIA EN CASO DE FALLAS DEL SISTEMA ACTIVO O PÉRDIDA DE DATOS

ELABORO: ZULMA JAIDITH ROJAS MATIZ **Ingeniera de Sistemas**	REVISA: STELLA MEDINA SOLANO **Jefe de Planeación**	LUIS IGNACIO BETANCOURT SILGUERO. **Gerente** APROBADO: **RESOLUCIÓN No.066 DEL 2020/01/29**
FECHA: 2020/01/23	FECHA: 2020/01/27	
Vo.Bo: MARTHA E. AMAYA C. **Oficina de Calidad**	FECHA: 2020/01/28	

CONTENIDO

INTRODUCCION

El Plan de Contingencia de información de la ESE "Solución Salud" es un documento que dispone los pasos para atender en forma adecuada, las fallas que se presenten en el Sistema de Información, Equipos de Comunicaciones, Equipos de Cómputo o desastres producto de eventos naturales u otros, a causa de algún incidente tanto interno como externo a Tecnologías de Información, con el fin de mantener activos los procesos críticos de la entidad ante la falla presentada y permita seguir operando. Teniendo en cuenta que la información es uno de los activos más importantes de la entidad, además de la infraestructura Informática y los procesos que el personal realiza continuamente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, Backup etc.) que soportan la información o datos críticos para la función de la entidad.

El Plan de Contingencia de la ESE SOLUCION SALUD elabora un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera establece medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o el hombre.

Es indispensable para el éxito del plan de contingencia, contar con personal capacitado y comprometido con la institución.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Formular un adecuado Plan de Contingencia, que permita la continuidad en los procedimientos informáticos de los sistemas de información, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda los sistemas de información de la ESE SOLUCION SALUD.

Determinar acciones y procedimientos a ejecutar en caso de fallas en la operatividad de los sistemas de información, debido a cortes de energía eléctrica, bloqueos en los aplicativos, corte o suspensión en la red de conectividad de internet, y demás situaciones que no permitan realizar el trámite de la historia clínica electrónica y financiera en el sistema de información Hosvital - HIS y Seven - ERP.

1.2 OBJETIVOS ESPECÍFICOS

Evaluar, analizar, prevenir o minimizar el daño permanente a los recursos informáticos en la ESE Dptal "Solución Salud" donde pueda ser suspendida completa o parcialmente la prestación del servicio.

Continuar con las funciones de las diferentes áreas de la ESE Dptal "Solución Salud", que se haya visto afectadas por falla o desastre.

2. ALCANCES Y RESPONSABLES

Definir acciones y procedimientos a ejecutar en caso de desastre, perdida de conexión o fallas de los elementos que componen los servicios informáticos

Es responsabilidad de todo el personal involucrado en los diferentes procesos y el personal de sistemas de información del nivel central.

3. GENERALIDADES

PLAN DE CONTINGENCIA: Es un conjunto de acciones, con una serie de procedimientos que nos orientan, a tener una solución alternativa que nos permita

restituir rápidamente los servicios de la entidad, ante situaciones de interrupción que puedan presentarse en los servicios ya sea de forma parcial o total.

La implementación del Plan de Contingencia de Sistemas de Información, incluye los elementos como: equipos, infraestructura, personal, servicios, sistemas de información y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la ESE Dptal "Solución Salud"

Por lo anterior se elabora este Plan de Contingencia para que el área correspondiente pueda supervisar la vigencia del mismo colocando en marcha soluciones en el momento de emergencia.

3.1 PLAN DE ACCIÓN

Realizar un levantamiento de los activos informáticos
Determinar cuál es la información crítica que se tiene que resguardar, determinando los servicios de cómputo, telecomunicaciones, Internet, que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus procesos normales.

Identificar un conjunto de amenazas.
Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto. Identificar el conjunto de amenazas que puedan afectar a los procesos informáticos, ya sea por causa accidental o intencional.

Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.

Se debe estar preparado para cualquier evento, verificando que dentro del área de sistemas cuente con los elementos necesarios para salvaguardar sus activos.

3.2 ETAPAS DE LA METODOLOGÍA

En el Plan de Contingencia Informático se establecen procedimientos preventivos para el manejo de casos de emergencia que se presenten en la ESE SOLUCION SALUD al padecer una situación anormal, protegiendo al personal, las instalaciones, la información y los equipos.

3.2.1 Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Mínimo: Es el que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.
Alto: Es el que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de 24 horas.

Crítico: Es el que afecta la operación y a las instalaciones, este no es recuperable en corto tiempo y puede suceder por que no existen normas preventivas o bien porque estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural.

3.2.2 Tipos de Contingencias de acuerdo al grado de afectación

- Instalaciones.
- En el mobiliario.
- En el equipo de cómputo del usuario final (procesadores, unidades de disco, impresoras, etc.).
- En Equipos Comunicaciones (Switch, Router, Servidores, Nodos, Líneas telefónicas).
- Información.

3.3 ANÁLISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

3.3.1 Factores de afectan la seguridad física y la infraestructura

Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales como los ataques provocados. Ambos riesgos tienen su origen de causas externas. De igual forma se encuentran las descargas o cortes eléctricos, los cuales pueden generar interrupción en las labores administrativas que pueden afectar la atención a los usuarios.

Riesgo: Es la vulnerabilidad de un activo o un bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgos:

- Riesgos Naturales (Mal tiempo, terremoto, inundaciones, etc.)
- **Riesgos tecnológicos** (Incendios eléctricos, fallas de energía y accidentes de transmisión y transporte).
- **Riesgos sociales** (Actos terroristas, desordenes, entre otros).

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

- **Grado de negatividad:** Un evento se define con grado de negatividad (Leve, moderado, grave y muy severo).
- **Frecuencia del evento:** Puede ser (Nunca, aleatorio, periódico o continuo).
- **Impacto:** El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- **Leves** (caídas de energía de corta duración, fallas en disco duro, equivocaciones, daño de archivos, acceso no autorizado etc.)
- **Severas** (Destrucción de equipos, incendios, inundaciones, daño de equipo, robos, etc.)

Tipos de contingencias de acuerdo al grado de afectación:

- En el mobiliario.
- En el equipo computo en general (Procesadores, unidades de disco, impresoras).
- En comunicaciones (ruteadores, nodos, líneas telefónicas).

3.3.2 Posibles daños

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución sea mediante robo o infidelidad del personal.
- Acceso no autorizado.
- Ruptura de las claves de acceso al sistema.
- Desastres naturales (terremotos, inundaciones, falla en los equipos de soportes causados por el ambiente, la red de energía eléctrica o el mal acondicionamiento de los equipos.
- Fallas del personal clave (enfermedad, accidente, renuncias, abandono del puesto de trabajo.)
- Fallas de hardware (fallas en los servidores o falla en el cableado de red, Router, etc.)

3.3.3 Clases de riesgo

- Incendio
- Robo común de equipos y archivos
- Falla en los equipos
- Acción de virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.
- Bajas Eléctricas.

3.4 FACTORES ASOCIADOS CON LA SEGURIDAD TÉCNICA INTEGRAL

Fallas, daños y/o deterioros por mal uso, fallas de mantenimiento y/u obsolescencia para switch, dispositivos, backup, PC, impresoras.

Corresponde al plan de contingencia minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno.

3.4.1 Factores de impacto de riesgo a las instalaciones de equipo de computadores, redes y otros

Fallas en el funcionamiento de los equipos o de los programas de protección, cuyo deterioro o mal uso pueden generar:

Grado de Impacto: Alto	Acción Correctiva
Daños en Discos duros, controladores de red, etc.	Contar con proveedores para disponer de reemplazo de piezas y repuestos de equipos que están para dar de baja.
Falla en los equipos de cómputo.	Realizar mantenimiento preventivo de equipos según el plan anual elaborado
Fallas en equipos de comunicaciones (switch, Router).	Contar con proveedores para disponer de reemplazo de piezas y repuestos de equipos que están para dar de baja
El daño de equipos de comunicaciones por fallas en la energía eléctrica, requiere contar con UPS redundantes que amplíen tiempo para apagar correctamente los equipos.	Se cuenta con planta de transferencia automática la cual en ocasiones presenta fallas y las UPS con que cuenta el Rack de comunicaciones requieren cambio de baterías.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Los equipos de escritorio no cuentan con una UPS dentro de la red de la entidad que soporta el guardado de la información temporalmente.

Se realiza mantenimiento preventivo a los equipos de usuario final de la entidad una vez al año, es necesario implementar estabilizadores a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.

Los cambios que sufran los servidores tanto en Hardware y Software pueden ser corregidos en la mayoría de los casos, sin embargo si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

3.4.2 Factores de impacto de riesgo virus informático

Grado de Impacto: Alto	Acción Correctiva
Software Antivirus	Cumple. La entidad cuenta con licencias de antivirus para cada uno de los equipos clientes y servidores. Se encuentra activa.
Sistemas es el área encargada de realizar la instalación del Antivirus.	Cumple.
Acceso restringido a Servidores para cambios en configuraciones de los mismos.	El personal del área de sistemas es el encargado de realizar las configuraciones respectivas a los equipos dentro del contexto para el cual fue contratado. (dba, jefe área, técnico de comunicaciones)
El área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Cumple. El personal autorizado del área de sistemas es el encargado de realizar la instalación del software con el que cuenta la entidad.
El antivirus no se actualiza periódicamente en cada equipo	Revisiones periódicas en los equipos cliente sobre la actualización del antivirus en el usuario final.

Se debe tener actualizado e instalado el antivirus en todos los equipos cómputo del usuario final de la entidad para prevenir daños por causa de un virus informático.

3.4.3 Factores de impacto de riesgo de información ingresada y eliminada en cada usuario

Grado de Impacto: Alto	Acción Correctiva
Se controla el acceso al sistema de red, a través de la creación de cuentas de usuario con el perfil indicado en cada uno de los aplicativos que maneja la	Se crean los usuarios de ingreso a los sistemas de información de acuerdo al perfil de ingreso a la entidad, reportado por el área de Recurso Humano o Jefe de área en su

entidad.	defecto.
La creación de usuario se realiza por el personal del área de sistemas autorizado	Por escrito (e-mail) llega la notificación al área de sistemas para la creación de los usuarios requeridos para el personal entrante. El área de sistemas diligencia el formato para la creación de cada usuario con el perfil solicitado.
El área de Recurso Humano debe comunicar al área de sistemas, cuando un funcionario sale a vacaciones o se retira de la entidad con el fin de desactivar el usuario	Es necesario que el área de Recurso Humano informe al área de Sistemas que personal sale a vacaciones o no continua en la entidad, con el fin de deshabilitar las cuentas al respectivo usuario por el tiempo de ausencia,
El personal de la entidad suele confiar su usuario y clave de acceso (personal) a compañeros de la oficina, sin medir la implicación de acceso no autorizado.	Cuando se entregan los usuarios por el área de sistemas, se explica al usuario la importancia de hacer uso de los usuarios asignados y que estos deben ser intransferibles. Se recalca la responsabilidad e importancia que ello implica, sobre todo para el manejo del software.
No se deshabilitan las cuentas de usuario del personal que se retira de la entidad de forma inmediata, en algunos casos se recurre a utilizar el usuario del funcionario ausente	Es importante que la oficina de recurso humano informe del personal que se retira de la empresa para realizar la des habilitación del usuario de forma inmediata.

3.4.4 Factores de impacto de riesgo de incendio, fuego o cortes de energía

GRADO DE IMPACTO ALTO	ACCIÓN CORRECTIVA
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma todos los pisos de la institución cuenta con un extintor debidamente cargados.	Se cumple. Se debe implementar un Sistema detección y extinción de incendios para Centro de Datos.
Se realiza la copia de seguridad diaria al servidor de bases de datos.	Cumple. Actualmente se realiza copia a la NAS y luego al Servidor en la Nube de los servidores de bases de datos de Hosvital-HIS y Seven-ERP
Daños en los equipos de trabajo de los usuarios por corte eléctrico.	No se tiene un plan de respaldo de protección de equipos de usuario final.
Daños en los Servidores por corte eléctrico.	Es necesario adquirir un sistema redundante de UPS y mejorar el sistema eléctrico del data center.
Daño en los equipos electrónicos de la red de datos por corte eléctrico.	Mejorar el sistema de UPS en el data center.

Pérdida de información por corte eléctrico.	Se debe mejorar los sistemas de respaldo, con el fin de evitar pérdidas mayores en la información por los cortes de energía.

Se requiere implementar un sistema automático de detención contra incendios en el data center de la entidad.

Las operaciones informáticas de la ESE SOLUCION SALUD se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, afectando los datos de alguna manera.

Actualmente de la ESE SOLUCION SALUD cuenta con una planta de transferencia automática que en algunas ocasionas presenta fallas en la transferencia y dos ups autorreguladas de 10kva cada una con un respaldo de autonomía de 5 minutos, la cual provee energía para los servidores que se encuentran en el Data Center lo que permite apagarlos servidores adecuadamente para evitar la pérdida de información.

3.4.5 Factores de impacto de riesgo de robo de equipos y archivos

GRADO DE IMPACTO MODERADO	ACCIÓN CORRECTIVA
No se tiene control personal particular que ingresa a la entidad. Tan solo se cuentan con algunas cámaras en el edificio de la entidad en caso de generarse algún incidente se revisarán. Para el personal de planta de la entidad se cuenta con un lector de huella para registrar el ingreso y la salida del personal.	Generar un sistema de control de acceso al personal particular de la entidad.
La salida y traslado de equipos en la entidad se realiza a través de un formato previamente diligenciado y firmado por el director del Centro de atención o en su defecto del área.	Cumple.
Hurto a mano armada	Se cuenta con seguridad privada.

La entidad debe contar con un sistema de ingreso y salida para el personal particular que llega a la entidad.

Establecer vigilancia mediante cámaras de seguridad la Dirección de la oficina de Sistemas, el cual registre todos los movimientos de entrada del personal.

Instalar identificadores mediante tarjetas de acceso.

Determinar lugares especiales, fuera del edificio central, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).

Contar, ya sea bajo contrato o mediante convenio, con un centro de cómputo alterno de características físicas y equipo de cómputo adecuado para darle continuidad a las operaciones críticas de la ESE SOLUCION SALUD, aún en forma limitada de cobertura y de comunicaciones.

3.5 EN CASO DE FALLAS DEL SISTEMA ACTIVO O PÉRDIDA DE DATOS

De acuerdo al incidente presentado al usuario final, debe reportar al área de sistemas a través de correo electrónico soporte.hosvital@esemeta.gov.co la falla presentada con evidencia fotográfica o video para ser atendida, ya sea vía telefónica o por asistencia remota.

De igual manera si el incidente presentado al usuario final es del módulo administrativo, la solicitud se debe reportar al área de sistemas a través de correo electrónico soporte.seven@esemeta.gov.co la falla presentada con evidencia fotográfica o video para ser atendida, ya sea vía telefónica o por asistencia remota.

El área de Sistemas evaluará el tipo de incidencia, si esta es de tipo 1, será solucionado por el área, en caso de ser incidencia de tipo 2, esta se registrará a través del Sac-Web del proveedor para ser asistida por ellos, para este tipo de solución tiene 24 horas para ser contestado por ellos. Si se considera necesario se iniciara proceso manual dependiendo el tipo de atención a realizar.

Una vez normalizada la operación del aplicativo HOSVITAL-HIS, SEVEN – ERP, PERSEO, SOPORTE LÓGICO puede seguir haciendo uso del mismo.

Continuar con la Operación de la Entidad: El Sistema de Información debe seguir en marcha una vez se hayan resuelto las inconsistencias presentadas, es importante retroalimentar a la Gerencia y los procesos involucrados para minimizar al máximo el riesgo y evitar que los problemas a nivel informático se presenten, ya que el sistema es totalmente transversal en todos los procesos que se manejan y a su vez la información es considerado como uno de los activos y más en el sector salud.

El manejo de Información Físico como Soporte: Una vez ingresado al sistema se tiene claro que la información que sea física o manual tiene la misma validez ante cualquier evento de revisión que solicite un ente control.

Tomar Acciones Correctivas y Preventivas para posibles Fallas: Jamás un riesgo es eliminado al 100% por tal motivo la parte residual siempre estará ausente y podrá ser motivo de fortalecimiento ante posibles acciones que se presenten posteriormente.

3.5.1 Determinar los tiempos de recuperación y la prioridad

TABLA DE PRIORIDAD Y TIEMPOS DE RECUPERACION

NOMBRE DEL SERVIDOR	PRIORIDAD DE RECUPERACIÓN (ALTA, MEDIA BAJA)	PRIORIDAD Y SECUENCIA DE RECUPERACIÓN	TIEMPO DE RECUPERACIÓN
NAS	Media	Media	48 Horas
Servidor en la Nube	Baja	Baja	12 Horas
Máquina Servidor de Dominio	Media	Media	48 Horas
Máquina servidor de Aplicaciones	Media	Media	48 Horas
Máquina servidor WEB	Media	Media	48 Horas
Máquina Servidor de Dase de Datos	Alta	Alta	72 Horas
Máquina Servidor de Dase de Datos	Alta	Alta	72 Horas

Situaciones críticas*:* Cuya afectación inutilice el área de sistemas y las instalaciones de la ESE SOLUCION SALUD.

Establecer un centro de cómputo alterno en 72 h. mínimo, con el equipo que se muestra en la tabla anterior, en red con cableado estructurado nivel 5E, bajo protocolo de comunicación TCP/IP. Se deberá contar con 1 línea telefónica y acceso a Internet.

Es recomendable tener un contrato para poder contar con un servicio de Almacenamiento en Internet, en el momento en que sea necesario, o de lo contrario contar con un convenio con alguna institución que pudiera ofrecer este servicio.

Para efectos de recuperación de la información, se cuenta con los procedimientos establecidos se anexan al presente documento.

Situaciones no críticas: que afecten solamente parte del equipo o alguno de los servidores.
Es necesario evaluar en primera instancia la gravedad del daño, si se determina que la reparación del equipo es viable en poco tiempo (8 h. Máximo), se procederá a su reparación por parte del técnico del área de sistemas.
En caso de habilitarse un servidor emergente, aún con capacidad menor al dañado, deberá quedar configurado con carga de aplicaciones y de información en máximo de dos días hábiles. De acuerdo con el personal del área de sistemas, en términos generales, este tiempo estimado, es en base a su experiencia.
Al concluirse la reparación del equipo, se regresara a servicio el servidor reparado, buscando realizar esto durante la noche o en un fin de semana, con el objeto de no entorpecer las actividades normales del personal usuario.

Daño o falla en Equipo de Comunicaciones. Se deberá sustituir de inmediato con equipo que se tenga disponible para estos casos, o en su defecto adquirir de urgencia el servicio con el proveedor especializado.

Falla de cableado: Para reparaciones mínimas el técnico del área de sistemas lo realizarán máximo en 2 h. Para efectuar el recableado o sustitución del tramo de cable dañado, se debe realizar un contrato de emergencia con algún proveedor.

Falla de tarjeta de red de estación de trabajo: Si se cuenta con refacciones en el stock se realizara la sustitución inmediata, lo que no debe tardar más de 3 h, de lo contrario se realizar un reporte a la dependencia afectada para que gestione la refacción.

Falla en Router: Es necesario evaluar en primera instancia la gravedad del daño, si se determina que la reparación del equipo es viable por parte el técnico del área de sistemas en poco tiempo (8h. Máximo) se gestionaran los repuestos necesarios, de lo contrario se contrataran los servicios de reparación externos o la compra del elemento, lo cual puede tardar entre 2 a 5 días.
Falla del sistema financiero y asistencial SEVEN – ERP, HOSVITAL - HIS: - Se deberá solicitar al proveedor la restauración del sistema, el cual por lo regular tarda 8 horas en restablecerse, a menos de que se trate de daño mayor, el cual puede tardar aprox. 48 horas.

Fallas de Internet:
Cuando se trate de fallas de acceso en Internet causadas por el proveedor del servicio, se deberá tener comunicación con el ejecutivo de cuenta para realizar el

reporte del daño y para establecer el tiempo en el que se estará sin servicio y buscando la solución más favorable para la entidad.

Requerimientos mínimos de recursos (software)

Las PC's para los usuarios y para personal de la Dirección de Sistemas Tecnológicos e Informáticos que operaría en las instalaciones alternas, deberá contar con la siguiente configuración mínima.

- Windows 8 Pro o Superior
- Office 2013 professional o Superior
- Antivirus
- Red y acceso a internet.

En el caso de que sea necesario restablecer Servidores dependiendo el uso es necesario contar con los siguientes programas actualmente dependiendo del servidor a instalar:

SOFTWARE - RESTABLECER SERVICIOS EN LOS SERVIDORES
Microsoft Windows Server 2012
Antivirus
SQL Server
Linux 3.10.0-862.6.3x86_64

3.6 MANEJO PARA LA CAPTURA DE LA INFORMACIÓN EN MOMENTOS CRÍTICOS

A continuación se indica la manera de llevar los procesos asistenciales como trámite de historias clínicas manuales en situaciones de falla de operatividad del sistema de información, estos son aplicables a todos los Centros de Atención que pertenecen a la ESE Solución Salud.

El aplicativo utilizado en la entidad para la digitalización de la historia clínica de los usuarios es Hosvital – HIS, en caso de una caída de energía o presentarse inconvenientes con el aplicativo, el personal asistencial en cabeza del director del centro de atención debe realizar el siguiente proceso.

3.6.1 Caída de Energía, Caída Masiva o Ventana de Mantenimiento del Aplicativo

Si pasado 20 minutos la energía no regresa debe iniciar el proceso manual, para ello debe descargar del sitio oficial de la entidad www.esemeta.gov.co los formatos indicados a continuación dependiendo de la atención a realizar:

Manejo de Módulos Historia clínica

1. CONSULTA EXTERNA:

1.1. MEDICINA GENERAL- ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial-Consulta Externa- Medicina General-FR-CE-01 Historia Consulta Externa.pdf

1.2. MEDICINA GENERAL HTA/DM ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-21 Historia Clínica de Riesgo Cardiovascular.pdf

1.3. AGUDEZA VISUAL ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial-Consulta Externa- Medicina General - FR-CE-02 Alteraciones de la Agudeza Visual.pdf

1.4. ODONTOLOGIA ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial-Consulta Externa- Odontología - FR-ODONT-08 Historia Clínica Odontologica.pdf

2. PROGRAMA PYP

2.1. PLANIFICACIÓN FAMILIAR ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-15 Atención en Planificación Familiar.pdf

2.2. CRECIMIENTO Y DESARROLLO ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-10 Alteraciones del crecimiento y desarrollo menor de 10 anos 01-22.pdf

2.3. CITOLOGIA: ruta – SGC- Formatos- Asistencial - Gestión De Calidad Asistencial (GQA) FR-GQA-47 CONSENTIMIENTO INFORMADO Y SOLICITUD DE CITOLOGIACERVICO UTERINA.docx y seguir con ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-13 Solicitud de Citologia.pdf y

2.4. CONTROL PRENATAL: ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-17 CLAP Materno Historia Clínica Materno Perinatal.pdf y seguir con la ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial - Gestión De Calidad Asistencial (GQA) FR-GQA-45 CONSENTIMIENTO INFORMADO CONTROL PRENATAL.docx

2.5. ATENCION DEL JOVEN ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-11 Historia Clínica Joven 10-29 Anos.pdf

2.6. ATENCION DEL ADULTO MAYOR ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial- Promoción y Prevención FR-PYP-20 Alteraciones del Adulto Mayor.pdf

3. HOSPITALIZACIÓN ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial-Hospitalización:

3.1. FR-HOS-01 Evolucion.pdf
3.2. FR-HOS-02 Ordenes Medicas.pdf
3.3. FR-HOS-03 Anotaciones de Enfermeria.pdf
3.4. FR-HOS-04 Signos Vitales.pdf
3.5. FR-HOS-05 Balance de Liquidos.pdf
3.6. FR-HOS-07 Curva Termica.pdf
3.7. FR-HOS-08 Tratamientos.pdf
3.8. FR-HOS-11 Fichas Medicamentos.pdf
3.9. FR-HOS-13 Epicrisis.pdf

4. URGENCIAS ruta http://www.esemeta.gov.co – SGC- Formatos- Asistencial-Urgencias

4.1. FR-URG-01 Triage.pdf
4.2. FR-URG-02 Atención de Urgencias 2015.pdf
4.3. FR-URG-03 Hoja de Gastos de Urgencias.pdf
4.4. FR-URG-04 Identificación y Resumen de Atención 2015.pdf
4.5. FR-HOS-13 Epicrisis.pdf

Cuando se reestablezca la energía se debe garantizar el debido ingreso de cada una de las atenciones realizadas manualmente en el aplicativo (Hosvital –HIS).

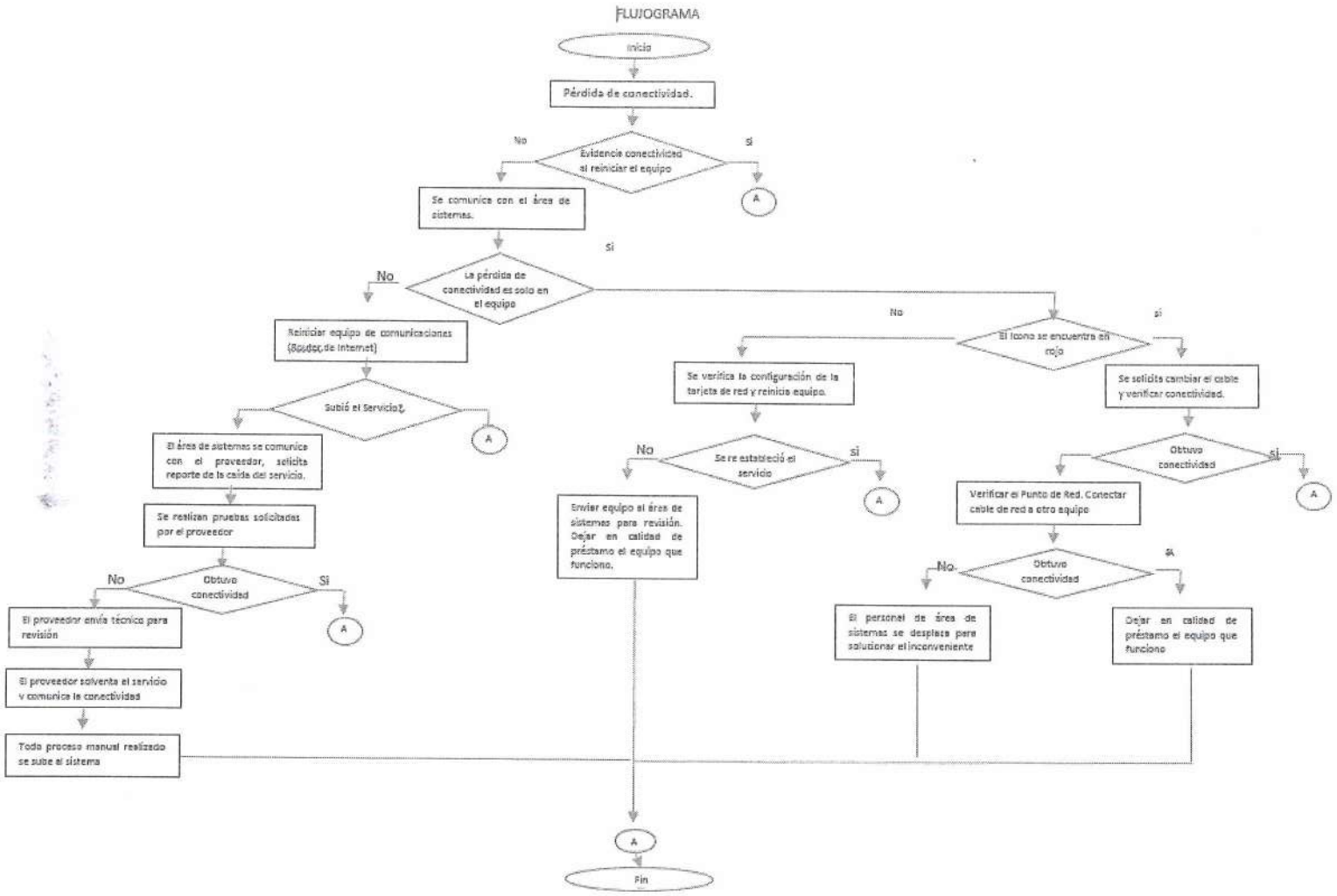
Manejo de Módulos Administrativos

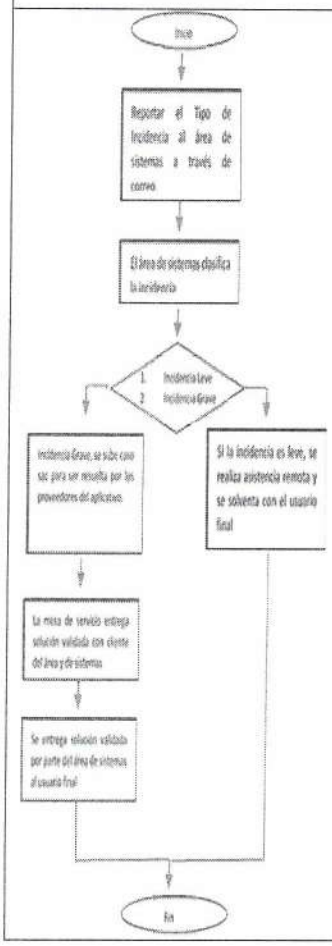
Los módulos administrativos como lo son: Presupuesto, Tesorería, Suministros (Almacén, Farmacia), Cartera, Contabilidad, Nomina, Archivo, son alimentados de la relación entre los demás módulos los cuales podrán continuar una vez se haya reestablecido el problema informático y una vez en funcionamiento se realizará el ingreso que se tiene en físico de la última copia de la base recuperada para llevar de forma consecutiva el ingreso de los documentos generados.

5. FLUJOGRAMA.

PROCEDIMIENTO	MANEJO PARA PÉRDIDA DE CONEXIÓN EN MOMENTOS CRÍTICOS				
ACTIVIDAD	**QUE**	**QUIEN**	**CUANDO**	**DONDE**	**COMO**
Ver flujograma 1	Evidencia pérdida de conectividad	Usuario centro de Atención	No pueda navegar o tenga red	Centro de Atención	Reiniciar equipo, si persiste el incidente, Enviar correo al área de sistemas: tecnico1.sistemasl@esemeta.gov.co, sistemas@esemeta.gov.co, o a través de llamada telefónica.
	Pérdida de conectividad solo en el equipo.	Usuario del centro atención	Se presente la	Centro atención, nivel central	Se verifica si perdida de conectividad se presenta solo en el equipo
	Validar Icono de internet	Usuario del centro de atención	Se presenta en rojo	Centro de Atención	Se debe cambiar el cable de red
	Se obtuvo conectividad	El equipo del centro de atención	El icono de internet cambie a estado normal	Centro de Atención	Ingresando a un sitio web
	Verificar el punto de red con otro equipo	Usuario Centro de Atención	Consiga equipo de cómputo para prueba	Centro de Atención	Conectando nuevo equipo al punto de red
	Obtuvo conectividad	Usuario Centro de Atención	Navegue el equipo de cómputo	Centro de Atención / Área de Sistemas	Dejando en calidad de préstamo el equipo que funciono, y enviando equipo con incidente al área de sistemas
	El icono de internet continua en rojo	Usuario Centro de Atención	Se presenta icono de internet en rojo	Equipo Centro de Atención	Enviar equipo al área de sistemas para su diagnóstico y revisión.
	Perdida de conectividad en todo el Centro de Atención	Centro de Atención	No tienen internet los equipos de cómputo del centro de atención	Centro de Atención	Reiniciar el router de internet
	Subió el servicio	Centro de Atención	Todos los equipos navegan e ingresan a los aplicativos	Centro de Atención	Se restablece el servicio
	El servicio continua caído	Proveedor de internet/Área de Sistemas	No se puede reestablecer el servicio de internet reiniciando el router	Centro de Atención	El área de sistemas se comunica con el proveedor, solicita reporte de la caída del servicio, se realizan pruebas solicitadas por el proveedor
	Se obtuvo conectividad	Centro de Atención	Todos los equipos navegan e ingresan a los aplicativos	Centro de Atención	Se reestablece servicio
	Servicio continua caído	Centro de Atención	No tienen internet los equipos de cómputo del centro de atención	Centro de Atención	El proveedor del servicio de internet envía técnico para su revisión, el personal técnico solventa el servicio y comunica la conectividad
	Servicio reestablecido	Centro de Atención	Equipos con navegación e ingreso a aplicativos	Centro de Atención	Todo proceso que se haya realizado manual en atención a usuarios, debe ser debidamente ingresado al sistema

Flujograma 1



PROCEDIMIENTO	MANEJO PARA LA CAPTURA DE LA INFORMACIÓN EN MOMENTOS CRÍTICOS				
ACTIVIDAD	DETALLE	QUIENES	CUANDO	DONDE	COMO
	Reportar el tipo de incidencia.	Área Asistencial.	Ocurrida la incidencia en el aplicativo	Centros de Atención	Enviar correo al área de sistemas: soporte.hosvital@esemeta.gov.co ,
	Tipo de atención 1. Tipo de Incidencia Leve 2. Tipo de incidencia Grave	Área de Sistemas	Se realice la lectura de la evidencia de la incidencia	Área de Sistemas	Revisión de evidencia por parte del área de sistemas, vía correo electrónico, remota o whatsapp
	Si la incidencia es leve	Área Sistemas	Se realice validaciones y pruebas con el usuario final	Área Asistencial	En línea a través de acceso remoto a la máquina del usuario.
	Si la incidencia es Grave	Área Sistemas	No se pueda dar solución por parte del área de sistemas	SacWebProveedor	Reportando el caso con evidencia del incidente al sac web del proveedor
	Incidencia Reportada como Grave	SacWebProveedor	Realice validaciones con el área de sistemas	Área de Sistemas	Entrega de solución después de validaciones y pruebas en ambiente del cliente

6. NORMATIVIDAD

Resolución 1995 de 1999, del Ministerio de Salud establece las normas para el manejo de la historia clínica.

Ley 23 de 1981. Artículos No 33, 34, 35. Po la cual se distan normas en materia de ética médica. Secreto profesional de la Historia Clínica. Regula archivos de las historias clínicas.

Decreto 3380 de 1981. Artículo 23. El conocimiento que de la historia clínica que tengan los auxiliares del médico o de la institución en la cual éste labore, no son violatorios del carácter privado y reservado de ésta.

Resolución 1832 de 1999. Artículo 3: Ajuste a la estructura de datos de identificación, consulta, procedimientos, hospitalización y urgencias.

Acuerdo 07 de 1994, Archivo General de la Nación de Colombia. Po el cual se adopta y se expide el Reglamento General de Archivos como norma reguladora del quehacer archivístico del país.

Acuerdo 011 de 1996, Archivo General de la Nación de Colombia. Por el cual se establecen criterios de conservación y organización de documentos.

Acuerdo 049 de 2000. Archivo General de Archivos sobre "Conservación de Documentos" del Reglamento General de Archivos sobre "Condiciones de edificios y locales destinados a archivos". Artículo 2: Condiciones Generales. Ubicación, aspectos estructurales. Artículo 4: Condiciones Ambientales y Técnicas.

7. CONCEPTOS BÁSICOS

Administración del Plan de Continuidad de Operación: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad

Problema de Continuidad de Operación: Es un evento interno o externo que interrumpe uno o más de los procesos de la Empresa. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.

Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución.

Riesgo: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.

Frecuencia: Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad.

Control: Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Resiliencia: Capacidad de una organización para resistir cuando es afectada por una interrupción.

Riesgo inherente: Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

Riesgo residual: Riesgo remanente tras la aplicación de controles.

Nivel de Criticidad. Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción: Incidente, bien sea anticipado o no anticipados los cuales pueden afectar el normal funcionamiento de las operaciones en alguna de las ubicaciones de la organización.

CONTROL DE CAMBIO

VERSIÓN No	DESCRIPCIÓN U ORIGEN DEL CAMBIO	APROBÓ	FECHA
1	Se elabora plan de contingencia en caso de fallas del sistema activo o pérdida de datos.	Gerencia	29/01/2020