HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

PLAN DE CONTINGENCIAS

Gestión de la Información

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

E.S.E.

2023

CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
Conmutador ***7333400*** * *Fax* ***7333408 y 7333409***
www.hosdenar.gov.co **mail:* ***hudn@hosdenar.gov.co***

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento contiene el estado de preparación actual del hospital universitario departamental de Nariño para responder ante un evento de interrupción producido por hechos naturales o por el hombre que pueda afectar la operación normal de los servicios informáticos, eléctricos y de comunicaciones, este plan está orientado a salvaguardar hardware, software, configuraciones y elementos complementarios que soportan la información o datos críticos para la función del hospital, en este documento se presentan los pasos que se debe seguir para dar una continuidad normal a los procesos y servicios de la entidad.

A través de este plan se pretende definir y cumplir metas que permitan al área de sistemas controlar el riesgo asociado a una contingencia, por esto se recomienda que este plan sea evaluado y actualizado de forma continua todos los años, considerando las nuevas situaciones de riesgo que se puedan presentar.

Este documento está dividido en tres partes, se inicia enunciando los riegos, identificando los objetos que deben ser protegidos y los daños que pueden sufrir, luego se evalúan, las posibles causas o sus posibles fuentes de daño y por último, se indica lo que se está haciendo actualmente para prevenir que esto ocurra y en caso de presentarse una interrupción inesperada, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

1. OBJETIVOS

1.1. OBJETIVO GENERAL.

Un Plan de Contingencia permite definir los riesgos y las acciones que garanticen una respuesta rápida y oportuna en casos de ocurrencia de incidentes de tipo natural y tecnológico. El objetivo es tomar las medidas necesarias para minimizar la probabilidad de que los riesgos se conviertan en una realidad y, si llegaran a ocurrir, posibilitar la reactivación de los sistemas de información y servicios informáticos que apoyan el cumplimiento de la misión de la entidad y aquellos procesos administrativos críticos.

1.2. OBJETIVOS ESPECIFICOS.

- Identificar los activos de información y los sistemas de información, considerados como críticos para el hospital.

- Identificar los riesgos y las amenazas a los que se encuentren expuestos los activos de información y los sistemas de información.

- Mitigar estos riesgos y amenazas a los que se encuentran expuestos los activos, sistemas de información y/o infraestructura informática.

- Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o posibles fallas ocasionadas.

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y/o infraestructura informática.

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información y/o infraestructura informática.

- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar que los objetivos de los procesos y procedimientos planteados en este, tengan los resultados esperados, aumentando los niveles de confiabilidad y disponibilidad de los sistemas de información y/o infraestructura informática.

1.3. ALCANCE.

El plan de contingencia del Hospital Universitario Departamental de Nariño E.S.E. cubre la infraestructura de telecomunicaciones, software, hardware y los sistemas de información y/o informática, se trata los riesgos, relacionados con la operación y los procesos de tecnologías de la información y/o informáticos, establecidas en los procedimientos de TI.

En este plan se abarca las etapas de notificación de la indisponibilidad del servicio, restablecimiento, evaluación y gestión.

2. MARCO LEGAL.

- Norma NTC – ISO 27001, Seguridad de la información.

- Decreto 2157 de 2017, por medio del cual se adoptan medidas generales para la elaboración del plan de gestión del riesgo de desastres de las entidades publicas y privadas en el marco del articulo 42 de la ley 1523 de 2012.

- Ley 46 de 1988, por medio de la cual se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres, articulo 3 numeral d) Los sistemas integrados de información y comunicaciones a nivel nacional, regional y local.

- Decreto Ley 919 de 1989, "Por el cual se organiza el sistema nacional para la prevención y atención de desastres y se dictan otras disposiciones", articulo 3 numeral d) Los sistemas integrados de información y comunicaciones a nivel nacional, regional y local.

- Guía Técnica Colombiana 202 de 2006, sistema de gestión de continuidad del negocio.

3. BIENES INFORMATICOS SUSCEPTIBLES DE UN DAÑO.

a) HARDWARE
- Servidores (ver anexo 1)
- Computadores de escritorio y portátiles (ver anexo 2)
- Impresoras multifuncionales (ver anexo 3)
- UPS y suministros de energía eléctrica (ver anexo 4)
- Redes de datos (ver anexo 5)

b) SOFTWARE DE APLICACIONES (ver anexo 6)

c) DATOS E INFORMACIÓN (ver anexo 7)

4. POSIBLES DAÑOS EN LOS BIENES INFORMATICOS.

a) HARDWARE.

SERVIDORES:

- Falla en disco(s) duro(s), memoria(s) RAM, procesador central, fuente(s) de alimentación y/o BOARD, tarjetas de red.

COMPUTADORES DE ESCRITORIO Y PORTÁTILES:

- Falla en disco duro, memoria(s) RAM, procesador central, fuente de alimentación y/o BOARD.

IMPRESORAS:

- Falla en el cabezal de impresión
- Efecto de cortocircuito en la bobina del cabezal
- Daño en el cable plano de señales
- Falla en la BIOS.

UPS:

- Daños en el sistema de rectificación
- Falla en las baterías
- Falla en el inversor
- Daño en el sistema de transferencia

REDES DE DATOS.

- Caída general de la red.
- Fallo del CORE principal de comunicación.

- Fallo de los switches de comunicación.
- Fallo del firewall de seguridad.

b) SOFTWARE.

SOFTWARE DE SISTEMA.

- Windows tarda mucho en iniciar y cerrar.
- La computadora se ha vuelto lenta.
- Bloqueos constantes del sistema.
- La PC se reinicia o apaga sola.

SOFTWARE DE APLICACIÓN.

- Falta el archivo DLL.
- Las aplicaciones que no se instalan adecuadamente.
- Las aplicaciones se ejecutan lentamente.
- Aplicaciones con comportamiento anormal.
- Certificaciones de seguridad desactualizadas.

c) DATOS DE INFORMACIÓN.

BASES DE DATOS.

- Eliminación parcial o total de las bases de datos.
- Falla en el acceso parcial o total a la información.
- Error en los índices de las tablas.
- Error en actualizaciones de seguridad del servidor (SO y sistema de gestión de bases de datos).
- Falla en el software que no permitan el acceso a las bases de datos.
- Hackeo.
- Falla en el proceso de elaboración de copias de seguridad.

5. POSIBLES FUENTES DE DAÑO.

Las posibles fuentes de daño que pueden causar la no operación normal del Hospital Universitario Departamental de Nariño son:

- ➢ Ingreso de personal no autorizado a:
- Instalaciones donde exista infraestructura tecnológica critica.
- Librerías, programas y datos.

- Ingreso de equipos no autorizados en la red del hospital (documento de referencia IRSGI-001 V02 INSTRUCTIVO SOLICITUD Y CREACION E IDENTIFICACION DE USUARIOS EN SISTEMAS DE INFORMACION).
- Ataque de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

- Desastres Naturales.
- Fallas de personal clave:

Se considera personal clave aquel que cumple una función vital dentro de una operación, el personal de la oficina de Gestión de la Información puede presentar los siguientes inconvenientes.

- Enfermedad.
- Accidentes.
- Renuncias.
- Abandono de sus puestos de trabajo.
- Sabotaje.

- Ausencia de fluido eléctrico.
- Incendios.
- Inundación en cuarto de servidores.
- Manipulación incorrecta de los sistemas informáticos por parte del personal del hospital.

6. MEDIDAS PREVENTIVAS PARA LAS POSIBLES FUENTES DE DAÑO.

6.1. PREVENIR INGRESO DE PERSONAL NO AUTORIZADO A INSTALACIONES DONDE EXISTE INFRAESTRUCTURA TECNOLÓGICA CRÍTICA (Tipo de riesgo - Medio).

Prevenir el ingreso de personal no autorizado a instalaciones donde existe infraestructura tecnológica crítica es crucial para garantizar la seguridad de la información y la continuidad de las operaciones. Se han establecido algunas medidas preventivas para prevenir y minimizar este riesgo:

- Controles de acceso físico: en el Hospital Universitario Departamental de Nariño E.S.E. se ha delegado en los funcionarios de la oficina de gestión de la información el manejo adecuado y correcto de las llaves, además las llaves se encuentran en un solo lugar y bajo la custodia y responsabilidad del funcionario líder de mantenimiento.

- Identificación y autenticación: el acceso restringido de personal sin autorización, tanto para los centros de cableado como para los lugares en donde se disponen de equipos de cómputo conectados a la red, para el ingreso en estas áreas el personal debe estar identificado con el carnet institucional, para empresas tercerizadas se deben identificar con los carnets autorizados por sus respectivas empresas.
- Zonas de acceso restringido: se han definido claramente las zonas de acceso restringido dentro de las instalaciones y se limita el acceso solo al personal autorizado.
- Monitoreo y vigilancia: se implementaron sistemas de monitoreo y vigilancia que registren el acceso a las áreas críticas y poder supervisar las actividades en tiempo real. estos sistemas son controlados por el personal de seguridad.
- Personal de seguridad: se cuenta con una empresa de seguridad capacitada y autorizada para supervisar el acceso y la seguridad de las instalaciones.
- Política de acompañamiento: el personal no autorizado debe estar acompañado por un empleado autorizado en todo momento mientras se encuentre en áreas críticas.
- Registros de acceso: se lleva un registro detallado de todas las personas que ingresan a las instalaciones, incluyendo visitantes, contratistas y empleados.
- Protección contra amenazas internas: se implementa políticas y medidas de seguridad para mitigar las amenazas internas, como el robo de datos, sabotajes o robo de hardware, por parte de empleados o contratistas deshonestos.

La implementación de estas medidas y el mantener un plan de contingencia efectivo y actualizado, hemos podido reducir significativamente los riesgos asociados con el ingreso de personal no autorizado, para más información en el manual de políticas de seguridad de la información (MNSGI-001 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION) se encuentra detallada una política de control de seguridad física.

6.2. PREVENIR EL INGRESO DE PERSONAL NO AUTORIZADO A LIBRERIAS PROGRAMAS Y DATOS (Tipo de riesgo - Medio).

Prevenir el ingreso de personal no autorizado a librerías, programas y datos es esencial para garantizar la seguridad de la información y proteger la integridad y confidencialidad de los recursos tecnológicos del Hospital Universitario Departamental de Nariño. Algunas de las medidas preventivas que se han implementado son:

- Gestión de accesos y autenticación: el ingreso a librerías, programas y datos del Hospital Universitario Departamental de Nariño E.S.E requiere de credenciales especiales y así poder tener conexión a los servidores y la información ver IRSGI-

001 - INSTRUCTIVO SOLICITUD Y CREACIÓN E IDENTIFICACIÓN DE USUARIOS EN SISTEMAS DE INFORMACIÓN.

- Segmentación de red: se utiliza la segmentación de red para dividir la infraestructura en zonas de confianza y asegurar que solo los usuarios autorizados tengan acceso a ciertas áreas.
- Control de privilegios: se ha limitado los privilegios de acceso a programas y datos solo a aquellos empleados que necesitan acceso para realizar sus laborales diarias.
- Gestión de contraseñas: se establecen políticas y procedimientos sólidos de gestión de contraseñas que incluyan la elección de contraseñas seguras, cambios regulares de contraseñas y la protección adecuada de las credenciales.
- Control de dispositivos extraíbles: se limita o prohíbe el uso de dispositivos de almacenamiento extraíbles, como unidades USB, para evitar la transferencia no autorizada de datos y posibles infecciones por virus cibernéticos.
- Control de aplicaciones: la instalación de aplicaciones se restringe para prevenir la ejecución de programas no autorizados en los sistemas de la organización.

La prevención del acceso no autorizado a librerías, programas y datos es fundamental para proteger los activos críticos, para mayor información consulta el manual de políticas de seguridad de la información (MNSGI-001 - MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION).

6.3. RESTRINGIR EL INGRESO DE EQUIPOS NO AUTORIZADOS EN LA RED DEL HOSPITAL (Tipo de riesgo - Medio).

El personal de la oficina de gestión de la información es cuidadoso de efectuar conexiones de computadores y dispositivos de terceros a las redes de datos y a los sistemas de información, para ello se implementó:

- Política de seguridad de la red: antes de proceder con la conexión de equipos, se exige poseer una herramienta antivirus vigente y que se actualice constantemente de forma inmediata, para proteger los activos de información.
- Autenticación de dispositivos: se registran equipos externos con autorización de la coordinación de G.I., además se restringe estos equipos a redes limitadas y controladas.
- Segmentación de red: la red del Hospital Universitario Departamental de Nariño E.S.E. se divide en segmentos o VLANs para aislar los sistemas médicos y críticos de los dispositivos no esenciales. Esto reduce el riesgo de que equipos no autorizados afecten los sistemas críticos.

- Bloqueo de puertos físicos: se han bloqueado físicamente los puertos de red no utilizados en las tomas de pared o en los conmutadores para evitar que se conecten dispositivos no autorizados.
- Gestión centralizada de dispositivos: la gestión centralizada de dispositivos no permite administrar y controlar de manera efectiva todos los dispositivos conectados a la red.

La seguridad de la red de la organización es crítica, para proteger la información del paciente y garantizar la continuidad de las operaciones médicas. Al implementar estas medidas preventivas y mantener un plan de contingencia actualizado, podemos reducir significativamente los riesgos asociados con el ingreso de equipos no autorizados a la red del hospital.

6.4. PREVENIR ATAQUE DE VIRUS INFORMÁTICO (Tipo de riesgo - Alto).

Dentro del manual de políticas de seguridad de la información (MNSGI-001 - MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION) se encuentra detallada una política de control de virus, en la cual se manifiestan las acciones que se realizan para prevenir un ataque informático, cabe resaltar que el Hospital Universitario Departamental de Nariño E.S.E. cuenta con la versión 2.20.11 de la solución de protección contra virus SOPHOS CORE AGENT, la cual cuenta con actualización permanente y soporte técnico por parte del proveedor local, la cual entrega una solución de seguridad corporativa más completa a fin de proteger cada equipo de cómputo que hace parte de la red corporativa del hospital.

Además, se capacita al personal para que se tengan muy presentes las siguientes iniciativas:

- Política de descargas: se establece una política prohibiendo la descarga de software y archivos de sitios web no autorizados o de dudosa procedencia.
- Educación y capacitación del personal: se incluye información y formación regular al personal sobre la seguridad informática y la conciencia de los riesgos asociados a los virus. Dirigida a que los usuarios aprendan a reconocer correos electrónicos de phishing, descargas de archivos sospechosos y enlaces maliciosos.
- Software antivirus y antimalware: se tiene y mantiene software antivirus y antimalware actualizado en todos los dispositivos y servidores. Los cuales se actualizan automáticamente para abordar las amenazas más recientes.
- Actualización de software: se mantiene todos los sistemas operativos, aplicaciones y programas actualizados con los últimos parches de seguridad.

- Copia de seguridad regular: se realiza copias de seguridad regulares de todos los datos críticos y del sistema HIS.
- Restricción de derechos de usuario: se limitan los derechos de usuario para minimizar la posibilidad de que se ejecuten programas maliciosos.
- Control de dispositivos extraíbles: se limita o prohíbe el uso de dispositivos de almacenamiento extraíbles, como unidades USB, para evitar la transferencia no autorizada de datos y posibles infecciones por virus cibernéticos.
- Filtrado de correo electrónico y navegación web: la herramienta de correo corporativo implementa filtros para el correo electrónico y los sitios web se bloquean mediante las herramientas de firewall físicos y lógicos. para reducir la exposición a enlaces de descarga de malware.
- Control de acceso a la red: se implementa medidas de control de acceso a la red para asegurar que solo los dispositivos y usuarios autorizados puedan acceder a la red de la organización.
- Segmentación de rojo: Se ha segmentado la red, para limitar la propagación de malware en caso de infección. Se aísla los sistemas críticos (servidores del HIS) de otros sistemas menos sensibles.
- Monitorización y detección de amenazas: La implementación de antivirus SOPHOS para la monitorización de seguridad de los equipos de computo internos y equipos de seguridad perimetral FORTINE para detección de amenazas e identificación a actividades sospechosas o malware.
- Políticas de contraseña segura: La implementación de procesos y procedimientos para la asignación de usuarios y claves (contraseñas) para el aseso a nuestro sistema de información hospitalario HIS, las cuales los usuarios deben cambiar regularmente.
- Gestión de vulnerabilidades: Se implementa pruebas de vulnerabilidad y penetración periódicas (PENTESTING), para identificar y abordar posibles puntos débiles en la seguridad informática.
- Revisión y mejora continua: Se revisa y mejora periódicamente las políticas y medidas de seguridad en función de las amenazas emergentes, se publica y comunica a las diferentes coordinaciones del hospital.

La prevención de ataques de virus informáticos es una parte fundamental de la ciberseguridad, Al implementar estas medidas preventivas, hemos reducido significativamente los riesgos asociados con virus informáticos, de igual forma proteger la integridad y continuidad de los sistemas de información.

6.5. PREVENIR DAÑOS DEBIDO A DESASTRES NATURALES (Tipo de riesgo - Medio).

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos en los centros de comunicaciones y de servidores, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico puedan generar mediante su caída la destrucción y/o interrupción del proceso normal de operación. Además, bajo el punto de vista de respaldo, tener claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, DVD´s, discos externos con información vital de respaldo, unidades de almacenamiento NAS y/o SAN, además contar con un almacenamiento externo como en la nube es de vital importancia para la organización.

Las medidas preventivas que se han incorporado en el plan de contingencia para reducir los riesgos asociados a desastres naturales son:

- Evaluación de riesgos: Se ha analizado los riesgos de desastres naturales que afectan al Data Center, y hemos podido identificar terremotos, inundaciones, incendios.
- Planificación y concientización: Se ha desarrolla un plan de contingencia detallado que aborda cómo la organización responderá a diferentes tipos de desastres naturales, este plan lo lidera el comité de Emergencias y desastres del hospital, el cual frecuentemente se socializa y comunica a todo el personal.
- Zonificación y evaluación de vulnerabilidades: Se mantiene en ejecución contratos de soporte y mejoras a las estructuras del hospital, al igual que mantenimientos permanentes.
- Infraestructura de seguridad: el hospital cuenta con un sistema de alarmas en caso de incendios al igual que un plan de emergencias ante desastres naturales.
- Respaldo de datos y sistemas: Se mantiene actualizado el procedimiento de copias de seguridad, con disponibilidad de almacenamiento para las copias de los sistemas críticos del hospital, se implementó copia cloud respaldo en la nube, además el protocolo de actualización del HIS especifica que el proceso de actualización se mantenga cubierto en cualquier eventualidad adversa.
- Suministro de energía de respaldo: Se implementa un sistema de respaldo de la red eléctrica, al igual se cuenta con una planta de alimentación eléctrica y un sistema de alimentación ininterrumpida (UPS) los cuales aseguran que los sistemas críticos continúen funcionando durante un periodo de tiempo, en los cortes de energía.
- Política de teletrabajo: Se implemento para pandemia Teletrabajo y permanece esta opción de trabajo de forma remota en caso de que las instalaciones físicas sean inaccesibles debido a un desastre.

- Seguro adecuado: El hospital cuenta con una póliza de aseguramiento por eventos naturales, la cual cubrirá los daños causados por desastres naturales, incluyendo daños a las instalaciones y la interrupción de las operaciones.
- Planes de evacuación y refugio: Se a desarrolla planes de evacuación por parte de la oficina de Emergencias y Desastres, para el personal y los visitantes en caso de un desastre.
- Comunicaciones de emergencia: Desde la oficina de comunicaciones se ha establecido protocolos de comunicación de emergencia, para informar al personal, a las autoridades y a las partes interesadas en caso de un desastre.
- Evaluación y mejora continua: La evaluación periódica del plan de contingencia, no permite identificar áreas de mejora, este se actualiza en función de lecciones aprendidas de simulacros y eventos reales.
- Educación y concientización: Se realiza despliegue y comunicados periódicos al personal y partes interesadas, educando y concientizando sobre la importancia de estar preparados y seguir el plan de contingencia en caso de un desastre, al igual que por parte de la oficina de Emergencias y Desastres se realiza simulacros de evacuación.
- Mantenimiento preventivo: Existen procedimientos de mantenimiento donde se especifican las reglas para realización de mantenimientos preventivo, cumpliendo con el cronograma de mantenimiento de equipos de computo y comunicaciones, servidores y equipo de respaldo del fluido eléctrico (UPS), garantizando el buen estado de funcionamiento.

La prevención de daños debido a desastres naturales se ha planificado y se viene mejorando continuamente. En este plan de contingencia se plantean varias políticas las cuales nos ayudan a minimizar los impactos y poder garantizar la seguridad y la continuidad de las operaciones en momentos de crisis.

6.6. PREVENIR FALLOS DEL PERSONAL CLAVE (Tipo de riesgo – Medio Alto).

Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización del software y elementos de soporte relevantes, esto permitirá mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones, enfermedades o pandemias.

6.7. PREVENIR DAÑOS EN AUSENCIA DE FLUIDO ELECTRICO (Tipo de riesgo - Medio).

El Hospital Universitario Departamental de Nariño E.S.E., cuenta con una planta de energía que entra a operar inmediatamente se presenta un corte en el fluido eléctrico, además se cuenta con 16 UPS que atienden los circuitos en donde se conectan los equipos de cómputo. En muchas partes también se encuentran UPS soportando la operación de los centros de cableado. Para más detalle ver el Anexo 04 de este documento.

En estos casos, se espera que no se presenten inconvenientes cuando los cortes de energía sean por pocos minutos (entre 1 y 10). Cuando los cortes de energía superen el tiempo de respaldo de las UPS se utilizarán las dos plantas eléctricas que tiene el hospital.

El proveedor de este servicio para hospital es Centrales Eléctricas de Nariño S.A E.S.P CEDENAR, esta empresa proporciona líneas telefónicas para reportar este tipo de casos, siendo estas: 733 69 00 en Pasto y la línea de atención al cliente 115 desde teléfono fijo o móvil.

En Fallas por tensión (Tipo de Riesgo –Alto), son fallas que se presentan como cambios bruscos en los picos de voltaje, causando problemas en las instalaciones internas, llegando a malograr equipos de cómputo si no se tiene las siguientes precauciones:

- Si hubiere fluctuaciones (flickers), constantes y prolongadas, proceder a apagar los equipos, previo aviso a los usuarios. Como medidas de seguridad ante la prevención se deberá contar con UPS, estabilizadores, supresores de picos, polo a tierra, etc.
- Llamar a la oficina de mantenimiento ext. 172 celular No. 318 538 3273 – 300 675 4743, para identificar si la falla es del sistema en general, o es un problema aislado en el tablero de alimentación de la sala de cómputo. Si la falla es originada en el sistema general, se debe esperar a que se normalice, para proceder a encender los equipos y conectar a los usuarios. Si la falla es originada por algún factor local, deberá, proceder a llamar a la oficina de mantenimiento para que el técnico en electricidad proceda a verificar los elementos del tablero de la sala de cómputo como son fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando esta falla; si no se detecta localmente se debe de proceder a revisar las conexiones, en la estación de donde se está independizando la energía (plantas de energía), revisar los bornes flojos u otros. Si aún no se detecta la falla, ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas, estufas, etc. y que se hayan conectado a la red de los equipos de cómputo por equivocación.

Por corte de Energía Imprevisto, Es el corte intempestivo del suministro de la energía eléctrica, ocasionado por algún factor externo, como son (corte de la línea de transmisión, accidentes, falla en los sistemas de protección, etc.).

Esta falla, tanto en el origen como al final (retorno de la energía) puede causar daños a los equipos de cómputo por lo que se debe seguir el siguiente procedimiento:

- Se activará la luz de emergencia en el equipo correspondiente.
- Revisar la carga del UPS que alimentan los equipos, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
- Llamar a la Oficina de Mantenimiento 172 celular No. 318 538 3273 – 300 675 4743, para identificar si la falla es del sistema general, o es un problema aislado, en el tablero de alimentación de la sala de cómputo.
- Por seguridad utilizar la energía que se tiene en los UPS para apagar los equipos en forma correcta.
- Si la falla es del sistema en general, se debe esperar a que se normalice, para proceder a encender los equipos y conectar a los usuarios.
- Si la falla es originada por algún factor local, deberá, proceder a revisar, los elementos del tablero de la sala de cómputo como son: fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando la falla, si no se detecta localmente se debe de proceder a revisar la conexiones, en la estación de donde se está independizando la energía (plantas de energía), revisar los bornes flojos u otros, Si aún no se detecta la falla ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc., y que hayan conectado a la red ocasionando un corto circuito, y que no permita, restituir la energía, en forma normal.
- Si la falla es en el sistema interconectado, se debe contactar con el proveedor de este servicio Centrales Eléctricas de Nariño S.A E.S.P CEDENAR, a las líneas telefónicas para reportar este tipo de casos, siendo estas: 733 69 00 en Pasto y la línea de atención al cliente 115 desde teléfono fijo o móvil, y se deberá esperar que se restablezca la energía, más un tiempo prudente de unos 15 minutos más aproximadamente, para que se estabilicé y se puedan levantar los sistemas.
- Si la falla es local proceder a la reparación, o reemplazo, de los componentes que causaron la falla, para esto se debe solicitar el apoyo al técnico de la oficina de mantenimiento 172 celular No. 318 538 3273 – 300 675 4743, (se recomienda tener fusibles, y una llave térmica de respaldo de acuerdo a la capacidad de su tablero). Una vez reparada la falla se debe de conectar la energía para ver el comportamiento, de esta y no encender los equipos de cómputo hasta después de 15 minutos aproximadamente después de la restitución de la energía).

6.8. PREVENIR INCENDIOS EN LOS BIENES INFORMATICOS (Tipo de riesgo - Medio).

Los equipos de cómputo pueden verse afectados por las altas temperaturas, vapor y productos de combustión provenientes de un incendio.

El Hospital Universitario Departamental de Nariño E.S.E. cuenta con 150 extintores, a continuación, se indica una tabla en la cual se detalla la cantidad y la clase de extintor.

CANTIDAD	CLASE DE EXTINTOR
33	PQS ABC de 30 lbs
24	PQS ABC de 20 lbs
34	PQS ABC de 10 lbs
1	PQS BC DE 10 lbs
6	PQS ABC de 5 lbs
2	PQS ABC de 150 lbs (Satélite)
30	Extintor CO2
20	Extintor agua des-ionizada

Además, se realizan inspecciones periódicas en las cuales se evalúa el estado de: gabinetes contraincendios, extintores, alarmas, pulsores de emergencia, pulsores contra incendio, lámparas para emergencias, megáfonos, inmovilizadores, circulación de pasillos, rutas y salidas de emergencia.

Si un incidente de estos se presenta proceder de la siguiente manera para minimizar el impacto:

- Si el inicio del incendio se produce en horas laborales, se procede a activar las alarmas contra incendios ubicadas en las instalaciones del hospital, activar el plan de emergencias provisto por los brigadistas y llamar a las líneas de los bomberos 602 733 29 29 línea de emergencia 119.
- Desconectar las fuentes de alimentación eléctricas (sin riesgo de exponer la vida).
- Si el tiempo lo permite y si la fuente del siniestro está lejos, pero se puede propagar hacia los equipos principales de computo (servidores) deberá retirar los equipos hacia un lugar seguro, discos o ultimas copias que tenga a la mano y (sin que esto signifique riesgo de exponer su vida).
- Se deberá proceder a sofocar el fuego utilizando el extintor correcto para el tipo de fuego.

6.9. INUNDACIONES EN EL CUARTO DE SERVIDORES (Tipo de riesgo Alto).

El cuarto de servidores del Hospital Universitario Departamental de Nariño E.S.E. al estar ubicado en el primer piso está expuesto a inundaciones repentinas que pueden afectar el funcionamiento de los sistemas informáticos que son de vital importancia, prevenir inundaciones en el cuarto de servidores es esencial para garantizar la continuidad de las operaciones de TI y proteger la infraestructura crítica en la organización, algunas medidas preventivas que se han incluido en un plan de contingencia para evitar inundaciones en el cuarto de servidores:

- Drenaje adecuado: en el área donde se encuentra ubicado el cuarto de servidores, manteniendo esté libre de suciedad o escombros que puedan obstruir el paso del agua.
- Ubicación adecuada: el cuarto de servidores está en un área elevada y alejada de zonas propensas a inundaciones, previniendo que este cerca de cuerpos de agua.
- Distribución de armarios: los servidores de servicios críticos, están ubicados a una altura mayor a 1 mt, según norma técnica de montaje de centros de datos.
- Impermeabilización: se ha impermeabilizado las paredes y el suelo del cuarto de servidores para evitar que el agua se filtre, asegurando que no haya grietas ni puntos débiles en la estructura que puedan permitir la entrada de agua.
- Sistemas de monitoreo: se implementó sistemas de video, para el monitoreo de posibles ingresos de agua, para alertar de manera temprana sobre la posible acumulación de agua en el área.
- Respaldo de datos y sistemas: se mantiene copias de seguridad (PRSGI-001 V02 PROCEDIMIENTO COPIAS DE SEGURIDAD DE LA INFORMACION) regulares de todos los datos y sistemas críticos en ubicaciones fuera del cuarto de servidores. Esto garantiza que los datos puedan recuperarse incluso en caso de una inundación catastrófica.
- Energía ininterrumpida: se ha implementado que el suministro eléctrico para los servidores esté respaldado por sistemas de energía ininterrumpida (UPS) y generadores de respaldo como plantas eléctricas, para evitar interrupciones en el caso de una inundación.
- Planes de evacuación y respuesta: se establece planes de evacuación y respuesta en caso de inundación. Se designa responsables y establece procedimientos para apagar sistemas de manera segura si es necesario evacuar el cuarto de servidores.

6.10. PREVENIR DAÑOS EN SISTEMAS INFORMATICOS POR MANIPULACIÓN INCORRECTA POR PARTE DEL PERSONAL DEL HOSPITAL.

El hospital cuenta con personal de soporte las 24 horas del día los 365 días del año, el cual está dispuesto a brindar en cualquier momento capacitación acerca del manejo de los sistemas informáticos al personal que lo requiera.

6.11. PREVENIR PERDIDA DE DATOS E INFORMACIÓN.

El hospital cuenta con una política de seguridad de la información la cual se detalla en el manual de políticas de seguridad de información (MNSGI-001) que se encuentra disponible en la página institucional, cabe resaltar que la información y los programas se encuentran almacenados en servidores, los cuales se protegen mediante claves de accesos.

6.11.1. SISTEMA DE RESPALDO Y RECUPERACIÓN.

Actualmente el hospital cuenta con 20 servidores funcionando las 24 horas del día, un servidor es un sistema encargado almacenar y transmitir la información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él, realizar copias de seguridad periódicamente en estos dispositivos es de vital importancia ya que la información que se transmite es múltiple y variada como archivos de texto, imágenes, videos, programas informáticos, bases de datos etc. Estas copias de seguridad se almacenan en discos duros en el área de sistemas. A continuación, se presenta una tabla en la cual está la frecuencia con la cual se realizan las copias de seguridad y los mantenimientos a cada uno de los servidores.

Pendiente listado por incluir

7. EJECUCION DE PLAN DE CONTINGENCIA.

7.1. EQUIPO DE CONTINGENCIA

El equipo de contingencia es el que ejecuta las tareas del plan de acuerdo con el diagnóstico del evento, el equipo de contingencia del área de sistemas cuenta con los siguientes integrantes:

NOMBRE INTEGRANTE	CARGO	E-MAIL	CELULAR	ROL

HENRY LUIS RODRIGUEZ CARDENAS	Coordinador Gestión de Información	hrodriguezc@hosdenar.gov.co	3155673127	Coordinador del plan de contingencia
JESUS EDUARDO ROSERO	Técnico Operativo de Gestión de la Información	jrosero@hosdenar.gov.co	3206331758	Responsable de recuperar hardware y software
WILLIAM ORLANDO SOLARTE DELGADO	Tecnólogo Contratista	wsolarte@hosdenar.gov.co	3015267648	Responsable de recuperar la red de datos
FELIPE VEGA RIVERA	Webmaster contratista	fvega@hosdenar.gov.co	3167262899	Responsable de recuperar portal Web y servidor mail
JAVIER PACHAJOA	Profesional provisional	jpachajoa@hosdenar.gov.co	3188089858	Responsable de recuperar bases de datos de finanzas
ORLANDO ARGOTY	Técnico Operativo de Gestión de la Información	oargoty@hosdenar.gov.co	3177507964	Responsable de restaurar copias de seguridad
ROBERTO EDUARDO FREIRE BURBANO	Profesional Contratista	rfreire@hosdenar.gov.co	3177201764	Responsable de realizar planeación
JESUS IVAN MAYA BASANTE	Técnico Contratista	jmaya@hosdenar.gov.co	3162890539	Responsable de recuperar servicios en servidores
ALEX MENESES	Técnico de Soporte contratista	ameneses@hosdenar.gov.co	3176486909	Apoyo a mantenimiento correctivo de Hardware y software
LUIS DARIO CRIOLLO	Técnico de Soporte contratista	lcriollo@hosdenar.gov.co	3152840992	Apoyo a mantenimiento correctivo de Hardware y software
OSCAR HERNAN ERAZO GAVILANES	Técnico de Soporte contratista	oerazog@hosdenar.gov.co	3102780480	Apoyo a mantenimiento correctivo de Hardware y software
EINAR ZAMBRANO	Técnico de Soporte contratista	ezambrano@hosdenar.gov.co	3165267760	Apoyo a mantenimiento correctivo de Hardware y software

7.2. PASOS PARA RECUPERAR EL HARDWARE.

a) SERVIDORES

Si el servidor posee un servicio critico este servicio debe ser migrado a otro equipo, en el caso de los servidores de alta disponibilidad los cuales posen el sistema de información gerencial estos operan de manera simultánea haciendo que las caídas sean menos probables, mientras se realiza el diagnóstico y se remplaza la pieza que está presentando fallas, si el servidor no posee un servicio critico el personal que opere este servicio será notificado para que no lo siga utilizando hasta que el equipo sea diagnosticado y reparado.

Servicios Críticos:

- Sistemas de información gerencial HIS.
- DHCP.

Otros Servicios:

- Resonador
- Tomógrafo
- Hunired
- Sevenet
- Portal Web
- Dinámica gerencial prueba
- Correo electrónico
- Huniweb
- sala de lectura
- Omnivista
- SOPHOS Antivirus
- Nube de Facturación
- Puertas UCS
- PACS

b) EQUIPOS DE COMPUTO E IMPRESORAS.

Si se trata de un servicio crítico el personal de sistemas deberá trasladar un computador o impresora de un servicio menos crítico para cubrir la situación, si se trata de un servicio NO crítico deberán esperar el diagnóstico y reparación del equipo.

Servicio Críticos

- Admisiones de Urgencias
- Unidad de cuidados intensivos (UCI)
- Quirófanos
- Cirugía General
- Facturación

c) UPS

La falla más común en las UPS se produce en las baterías por ello se realizan revisiones periódicas de su funcionamiento, pero en caso de que alguna pieza del hardware llegase a fallar se realiza un bypass el cual se deja la carga que estaba conectada a la UPS soportada en la línea comercial, mientras se realiza el diagnóstico y remplazo de la pieza que presenta falla.

7.3. PASOS PARA RECUPERAR EL SOFTWARE.

a) SOFTWARE DE APLICATIVOS:

Los aplicativos que se están utilizando en el hospital se encuentran almacenados en el servidor denominado HOSPITALP1 con dirección IP 172,16.50.1, estos se encuentran en carpetas compartidas disponibles para cualquier persona que se conecte a la red del hospital, si algún aplicativo llegase a fallar, la persona encargada del desarrollo de software deberá restablecer el servicio en caso de que el aplicativo haya sido desarrollado por la entidad, de lo contrario deberá contactarse con los desarrolladores externos y solucionar el problema.

7.4. PASOS PARA RECUPERAR INFORMACIÓN.

Las copias de seguridad se almacenan en el servidor HOSPITALP1-1 con dirección IP 172.20.100.8 en caso de pérdida total o parcial de información, el equipo de contingencia tiene una persona encargada de restaurar las copias de seguridad, esta persona será notificada y se encargara de identificar la información que se perdió e informar a cada una de las áreas para que la información perdida sea nuevamente ingresada en el sistema.

7.5. ACTIVIDADES QUE SE REALIZARÁN MIENTRAS SE REINICIA EL SERVICIO.

El tiempo que se demore en restablecer el servicio dependerá del daño que se haya generado, por lo tanto, todas las áreas del hospital deberán continuar sus actividades utilizando recursos logísticos como listados, calculadora, factura entre otros. Por ejemplo, para los usuarios que deben recaudar dinero, deberán emplear facturas que deben contener la identificación del usuario, nombre completo del usuario, fecha de atención, valor por cada servicio y debe ser firmado por el paciente o acompañante y se le hace entrega de una copia.

En el caso de NO haber necesidad de recaudo de dinero, la información deberá ser ingresada en los diferentes formatos establecidos por la entidad como por ejemplo el formato de historias clínicas el cual debe estar disponible en los servicios donde se requiera y una vez se restablezca el sistema, la información debe ser ingresada inmediatamente.

7.6. CÓMO SE NOTIFICA Y EVALÚA LA CONTINGENCIA CUANDO SE PRESENTA.

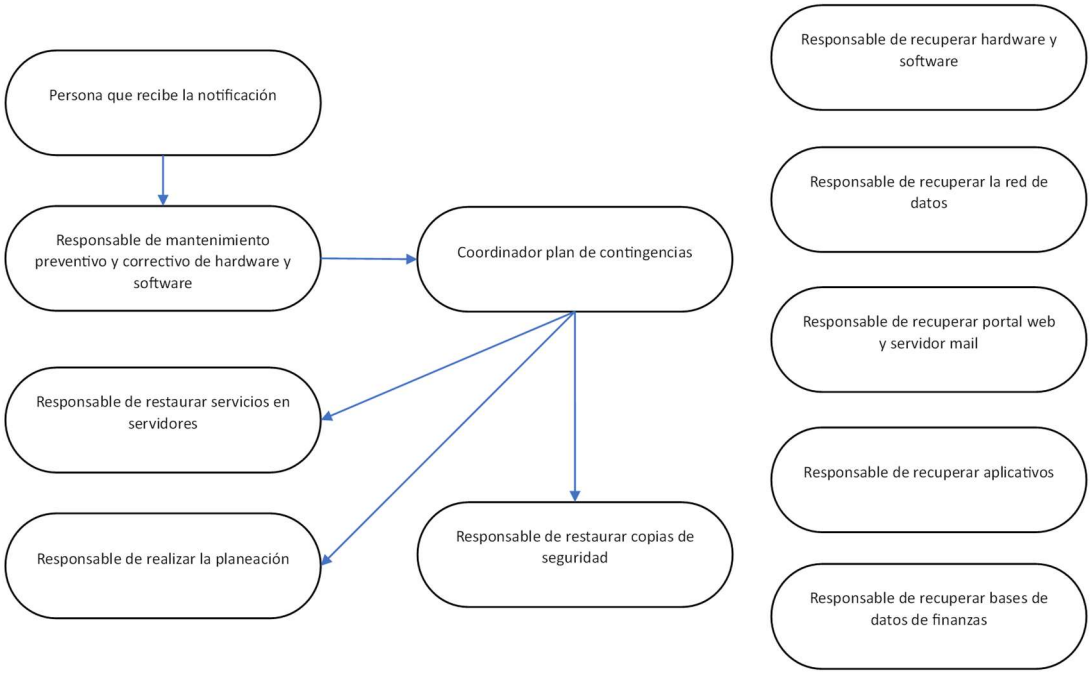
Quien notifica la contingencia será el funcionario que detecte cuando se presente alguna(s) de las posibles causas enunciadas o no en este documento. Esto de forma inmediata activara el Plan de Contingencia, a fin de eliminar los elementos que están interfiriendo con el normal funcionamiento de las aplicaciones y la prestación de los servicios.

La notificación pueda hacerse en forma verbal, o telefónicamente, o mediante medios electrónicos como email, mensajería instantánea o redes sociales. Para lo cual pueden usar los siguientes datos:

- Teléfono Dirección de Sistemas de Información: 7333400, extensión 488.
- E-mail mesa de ayuda: soportehudn@hosdenar.gov.co.
- E-mail Dirección de sistemas de Información: sistemashudn@hosdenar.gov.co.
- Línea celular de soporte 24/7 No. 318 538 3273.

Cualquier integrante de la oficina de Gestión de la Información, recibirá el mensaje e iniciará la cadena de llamado.

7.7. CADENA DE LLAMADO.



HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

ACREDITACION EN SALUD

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

SIMULACRO DEL PLAN DE CONTINGENCIA GESTION DE LA INFORMACION 19-09-2023

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

SIMULACRO DEL PLAN DE CONTINGENCIA GESTION DE LA INFORMACION 19-09-2023

Introducción

El presente documento indica los pasos que se deben realizar ante una posible caída del sistema de información Hospitalario HIS, debido a fallas en hardware, software o red de datos, actualmente el hospital cuenta con dos servidores, con sistema operativo Windows Server 2019 Estándar Edition – 64 bits, 2 Procesadores Common KVM Processor 2.19 GHz, Memoria RAM física instalada 192 GB en el cual se almacena la base de datos del sistema de información dinámica gerencial, igualmente se debe tener en cuenta otras causas como son la caída de la red de datos.

Objetivos:

- Identificar la ruta de almacenamiento de las copias de seguridad y los responsables de cada uno de los procesos.
- Conocer los pasos que se deben realizar ante esta contingencia.
- Medir los tiempos de respuesta de cada uno de los diferentes pasos estipulados en el simulacro.
- Conocer el tiempo total que estaría el hospital sin el servicio del Sistema de Información Hospitalario HIS.

Pasos a seguir:

1 – El Personal de mantenimiento recibe la notificación y verifica el grado del daño reportado, y según el tipo o grado se continua con el paso siguiente.

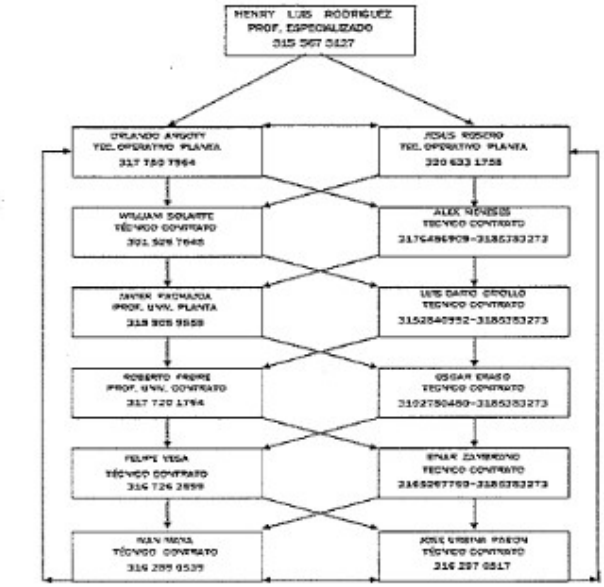
2 – Activar la cadena de llamado PLSGI-002 AN-01 y el Proceso en unà Eventual Caida del sistema de información Hospitalario HIS, en el cual se se enumeran los pasos a seguir en esta contingencia.

CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
Conmutador ***7333400*** ** Fax* ***7333408 y 7333409***
www.hosdenar.gov.co **mail:* ***hudn@hosdenar.gov.co***

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

	CADENA DE LLAMADO – GESTIÓN DE LA INFORMACIÓN	CÓDIGO: PLGSI-002 AM-01	FECHA DE ELABORACIÓN: 27 DE OCTUBRE DE 2020
			FECHA DE ACTUALIZACIÓN: 15 DE ENERO DE 2022
		VERSIÓN: 02	HOJA 1 DE 1



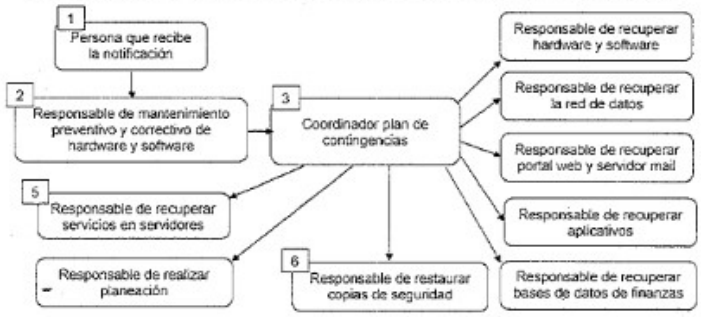
ROBERTO FREIRE Realizado por: PROF. UNIVERSITARIO GESTIÓN DE LA INFORMACIÓN	HENRY RODRIGUEZ Revisado por: PROFESIONAL ESPECIALIZADO GESTIÓN DE LA INFORMACIÓN	NELSEN ALVEAR Aprobado por: GERENTE	15-01-2022 Fecha de aprobación

VERSIÓN	FECHA	DESCRIPCIÓN
01	27-10-2020	Creación del documento
02	15-01-2022	Actualización

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

Proceso en una Eventual Caída del Sistema de Información Hospitalario HIS.



3 – Notificar a los coordinadores de las áreas afectadas, ademas se informara que se encuentran habilitados los formatos de contingencia HISTORIA CLINICA y formato de contingencia MIPRES, estos se encuentran habilitados en Aplicativos HUDN y reposaran en el área de estadistica para ser duplicados en caso de un fallo en la red de datos.

4 – Notificar al personal que esté utilizando en ese momento el sistema de información hospitalario HIS, para que guarde la información y reinicie la aplicación cuando se le notifique de la restauración del sistema.

CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
*Conmutador **7333400** * Fax **7333408 y 7333409***
www.hosdenar.gov.co** *mail: **hudn@hosdenar.gov.co

CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
*Conmutador **7333400** * Fax **7333408 y 7333409***
www.hosdenar.gov.co** *mail: **hudn@hosdenar.gov.co

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

5 – Identificar la última copia de seguridad generada, actualmente las ultimas copias de seguridad se almacenan en un sistema de almacenamiento NAS con IP: 172.20.100.145 Y también se respaldan el un almacenamiento en la nube del proveedor Google Drive.

6 – Descomprimir y Restaurar la Base de datos en el mismo servidor donde se encuentran almacenados los últimos backups.

7 – Cambiar dirección IP al servidor de respaldo, se debe cambiar la dirección IP, estos pasos se detallan mas a fondo en el Protocolo de actualización del HIS.

8 – Verificar si se puede acceder correctamente a Dinámica Gerencial Hospitalaria desde cualquier equipo conectado a la red del hospital.

9 – Realizar registro de datos en el sistema de información DGH, para verificar que se almacenen correctamente

10 – Notificar a los coordinadores de las diferente areas y al personal del hospital que se retablecio el sistema de información.

11 – En caso de que la contingencia sea por fallas en la red el personal de apoyo y soporte de la oficina de GI debe identificar la posible causa de caida de la red.

12 – Identificado el problema se procede a cargar la ultima compilación del sistema de información hospitalario HIS, en un servidor alterno, realizado esto se procede a efectuar los pasos 7 al 10.

HENRY LUIS RODRIGUEZ CARDENAS
Coordinador
Gestión de la Información

JESUS IVAN MAYA
Técnico de servidores
Gestión de la Información

CALLE 22 No. 7 - 93 Parque Bolivar - San Juan de Pasto / Nariño
Conmutador ***7333400*** ** Fax* ***7333408 y 7333409***
www.hosdenar.gov.co **mail:* ***hudn@hosdenar.gov.co***

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

LISTA DE CHEQUE SIMULACRO PLAN DE CONTINGENCIA GESTION DE LA INFORMACION 19-09-2023

Pasos: -

Ítem	Descripción	Responsables	Hora inicio	Hora Final
1	Notificación personal de soporte	Einar Zambrano	8:30 pm	8:35 pm
2	Evaluación grado del daño	Einar Zambrano	8:36 pm	8:50 pm
3	Notificación de soporte a coordinación GI	Einar Zambrano /Ing. Henry Rodríguez	8:51 pm	8:52 pm
4	Notificación coordinación a responsable de servidores	Henry Rodríguez/Iván Maya	8:53 pm	8:57 pm
5	Notificación de coordinación al personal de copias de seguridad	Henry Rodríguez/Felipe Vega	8:58 pm	9:02 pm
6	Notificación de coordinación a las diferentes áreas del HUDN – Urgencias, Hospitalización, Ginecología, Cirugía general, UCI's, Laboratorio, Servicio farmacéutico.	Ing. Henry Rodríguez	9:03 pm	9:14 pm
7	Notificación al personal que en ese momento este utilizando el HIS.	Einar Zambrano	9:02 pm	9:18 pm
8	Identificación de la última copia de seguridad	Felipe Vega/Iván Maya	9:15 pm	9:21 pm
9	Mover la copia de seguridad al servidor de respaldo	Felipe Vega/Iván Maya	8:58 pm	10:18 pm
10	Restaurar base de datos	Iván Maya	10:18 pm	11:18 pm

HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E.

¡Trabajamos por mi Nariño,
tu salud,
nuestro compromiso!

11	Cambio de dirección IP 172.20.100.145 por 172.16.50.1 del nuevo servidor.	Iván Maya	11:18 pm	11:20 pm
12	Verificación acceso correcto a HIS.	Einar Zambrano - Iván Maya	11:20	11:24
13	Ingreso de datos de prueba en el HIS	Orlando Argoty/Iván Maya	11:24	11:31
14	Notificación al personal que el servicio queda restablecido	Einar Zambrano – Iván Maya	11:31	11:36

Análisis de resultados

1. El simulacro inicio a las 8:30 p.m. y termino a las 11:36 p.m., esto quiere decir que el tiempo que tomo entre la notificación del daño y la notificación de restablecimiento del servicio fue de 3 horas y 6 min, cabe resaltar que estos son ideales debido a que el personal necesario para ejecutar el simulacro se cita por la actualización del sistema de información hospitalario HIS.
2. El tiempo que tarda en mover la última copia de seguridad no siempre va a ser el mismo este puede aumentar en tiempo debido a que el tamaño de la copia aumenta con el tiempo y también es crucial contar con una buena trasferencia en la red de datos.
3. La pérdida de información es inevitable ya que el tiempo entre la notificación del error y la notificación a todo el personal de hospital que en ese momento está utilizando dinámica gerencial es de 33 min, lapso de tiempo que el sistema no permitirá guardar datos, si estos datos no son almacenados en otro medio se perderán.

Conclusiones

- Los tiempos de respuesta por parte del equipo de apoyo y soporte de la oficina de GI, aun es alto porque en la práctica se pueden encontrar varios factores que impidan el restablecimiento del sistema en poco tiempo, a pesar de cotar con un sistema de alta disponibilidad HD.

Control de cambios:

E: Elaboración del documento.
M: Modificación del documento.
X: Eliminación del documento.

Versión	Control de cambios	Información de cambios					Acto Administrativo de adopción (si aplica)	Fecha de creación/Actualización
		E	M	X	Actividades o justificación de cambios	Elaboró/Actualizó		
01	Creación y aprobación del documento	X			Se crea Plan de contingencia de Gestión de la Información del Hospital Universitario de Nariño ESE.	Roberto Freire B. Ingeniero de Sistemas contratista G.I.		
02	Actualización controles y documentación.		X		Se controles de posibles amenazas y sus respectivos controles y salvaguardas.	Roberto Freire B. Ingeniero de Sistemas contratista G.I.		10/07/2023