TRD. 322.1.28.126

PLAN DE CONTINGENCIA GESTION DE LA INFORMACION

Responsables:

Ing. Yanet Moreno

Wilmar Lizcano

Leidy caterine Mejia

TRD. 322.1.28.126

GESTION DE LA INFORMACION HOSPITAL DEL SARARE ESE

INTRODUCCIÓN

El Plan de Contingencia es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y de las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y Organizativas necesarias para garantizar la continuidad de las operaciones de la institución. Así mismo, este plan de contingencias sigue el conocido ciclo de vida iterativo "plan-do-check-act", es decir, "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la entidad. El plan de contingencias deberá ser revisado semestralmente. Así mismo, es revisado/evaluado cuando se materializa una amenaza. El Plan de Contingencia permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada. Ha sido elaborado tomando como base, la Metodología ITIL (INFORMATION TECNOLOGY INFRASTRUTURE LIBRARY) - Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información. El Plan de Contingencia debe involucrar a los actores relevantes. Este plan de trabajo considera evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos.

TRD. 322.1.28.126

ORGANO RESPONSABLE: Gestión de la Información

1. ETAPAS DEL PLAN:

a) Análisis de Riesgos
b) Plan de Respaldo
c) Plan de Recuperación
d) Plan de Mantenimiento
e) Plan de Entrenamiento

2. DEFINICIÓN:

Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de la organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa. Esta clase de plan, por lo tanto, intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución.

3. DIAGNOSTICO SITUACIONAL: Actualmente el Hospital del Sarare cuenta con los siguientes Equipos de Cómputo:

a) Hardware:
1) 271 UPS
2) 390 Computadoras
3) 84 Impresoras
4) 50 Escaner
5) 30 Laptop
6) 04 tablets

b) Comunicaciones:
1) 04 acces point
2) 20 Switch de 24 puertos
3) 14 Servidores

c) NECESIDAD DE REALIZAR EL MANTENIMIENTO

Es necesario por tanto 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.

Debe contemplar los planes de emergencia, backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

5. FINALIDAD

Tener un Plan de Contingencias lo más completo y global posible. Definir las normas y procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los Sistemas de Información y Comunicación del Hospital, de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos.

TRD. 322.1.28.126

6. OBJETIVO GENERALES

Un Plan de Contingencia y Seguridad de la Información permite prever los riesgos a los que estará sometido el sistema de información que se va a implementar. El objetivo es doble: Por un lado, tomar las medidas necesarias para minimizar la probabilidad de que dichos riesgos se conviertan en una realidad y, por otra parte, si esto ocurriera, posibilitar que el sistema pueda responder sin que ello suponga un grave impacto para su integridad. Este presente Plan de Contingencia y Seguridad, involucra a toda la entidad directa o indirectamente. De este modo, es válido en cuanto se produce con la aprobación de todas las partes implicadas, con la total asunción de responsabilidad que a cada una pudiera corresponderle.

7. OBJETIVO ESPECÍFICOS

a) Proteger la vida de las personas inherentes a los servicios informáticos de la entidad.

b) Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de la entidad.

c) Proteger la propiedad de la entidad y otros activos.

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

e) Proteger al sistema de información de pérdidas irreparables de información procesada.

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

g) Alcanzar una alta disponibilidad, es decir, impedir que se produzcan fallas en los sistemas, que dificulten el normal funcionamiento de nuestra Institución.

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

i) Impedir que el daño material de cualquier soporte de información, conlleve o no a la pérdida de información: máquinas, instalaciones, líneas de comunicación etc.; además de otros objetivos como establecer las medidas organizativas y técnicas para asegurar la confidencialidad, integridad y disponibilidad de la información y el soporte informático en nuestra entidad.

8. LOGRO QUE SE ESPERA ALCANZAR

Brindar un óptimo funcionamiento y proteger toda la información que se procesa día a día la misma que es almacenada en los servidores que utiliza el Hospital.

9. AMBITO DE APLICACIÓN: Hospital del Sarare ESE.

10. ACTIVIDADES A REALIZAR:

- ✓ El Plan de Contingencia y Seguridad de la Información

TRD. 322.1.28.126

Se elabora desde el área de Gestión de la Información en coordinación con las sedes internas y externas ligadas a la entidad. El Plan de Contingencia está diseñado para ser aplicado tanto en la Sede principal de la entidad como en La sede Unap de la Institución, involucrando al personal y equipos que intervienen en el mantenimiento de la función informática en nuestra institución y contemplen el software base y las aplicaciones informáticas, así como controlar los accesos a áreas de uso restringido y el hardware. Los resultados esperados son establecer los controles necesarios en la función informática y en el uso de las aplicaciones con el fin de garantizar la integridad y confidencialidad de la información y el soporte informático ante cualquier siniestro que pudiera ocurrir.

✓ Esquema General:

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos las instalaciones, equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en el Plan Contingencia se hará un análisis de los riesgos (Antes), cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema (Durante). Pese a todas las medidas se seguridad con las que cuenta la institución puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres (Después), el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible. Comenzaremos por identificar los tipos de riesgos y los factores para proceder a un plan de recuperación de desastres, así como las actividades previas al desastre, durante y después del desastre.

✓ Definiciones de Términos Empleados

i) Contingencia: Interrupción, no planificada, de la disponibilidad de recursos informáticos.
ii) Plan de Contingencia: Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
iii) Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.
iv) Impacto: El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, en:
   a. (1) Impacto Alto: Se considera que una actividad crítica tiene impacto alto sobre las operaciones de la entidad cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.
   b. (2) Impacto Medio: Se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones de la entidad por un tiempo mínimo de tolerancia.
   c. (3) Impacto Bajo: Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la entidad.

d) Análisis e Identificación de Riesgos En la institución, se ha identificado los siguientes tipos y factores de riesgos:

TIPOS DE RIESGOS	FACTORES DE RIESGO
Falla de equipo	Alto
Fallas por tensión	Alto
Accesos no autorizados	Alto
Acción de Virus	Medio

TRD. 322.1.28.126

Terremoto	Medio
Fuego	Medio

1. **En caso de Infección por Acción de Virus (Tipo de Riesgo –Medio)** La entidad cuenta con el antivirus NOD32 para los servidores y para las estaciones de trabajo; asimismo a través de la red se hacen las actualizaciones del antivirus hacia las máquinas correspondientes. Sin embargo, en caso de infección masiva de virus se debe de seguir el siguiente plan de contingencia:

1. Si la infección es vía red a los Servidores y PCS, proceder de la siguiente forma:

✓ Revisar las alertas que envía el antivirus y ver el tipo de virus que se está propagando detectando el origen del virus. A su vez desconectar de la red el equipo que está infectado y que está reenviando el virus.

✓ Comprobar si tiene carpetas compartidas en forma total y proceder a no compartirlas.

✓ Explore su equipo con las opciones que proporciona NOD32.
✓ Proceder a limpiar los archivos con la opción de: LIMPIAR o CLEAN INFECTED FILES NO CON DELETED por que esta opción podría borra archivos del sistema operativo, quedando inutilizada la máquina.

✓ Una vez limpio el equipo, proceder a realizar una copia de Seguridad sólo de la Data. Si no se lograra limpiar en forma satisfactoria, el equipo, porque los archivos del sistema operativo han sido dañados se procederá a formatear el disco reinstalándole el sistema operativo y transfiriendo la data de seguridad, que se tiene en caso de servidores y de los archivos personales en caso de PC y/o Servidor de Archivos en donde se custodia la data de los usuarios.
2. Si la infección es por lista de correo proceder de la siguiente forma:

1. Contactar a la empresa que nos provee el servicio de correos.
2. Reportar en la mesa de ayuda sobre el inconveniente que se pueda presentar.
3. Realizar las acciones de mejora que la mesa de ayuda de la empresa de servicio de correo nos propone.

2. **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:

1. 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.

2. Llamar a Oficina de Mantenimiento para identificar si la falla es del sistema 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

TRD. 322.1.28.126

localmente se debe de proceder a revisar las conexiones, en la subestación de donde se está independizando a 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.

2) 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 de 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, 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 originada en el sistema general, se debe esperar a que se normalice, (siempre en coordinación), 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 subestación de donde se está independizando la 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 (general) se deberá esperar que restituya la energía, más un tiempo 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 de solicitar el apoyo al técnico de la oficina de mantenimiento, (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).

3) En caso de Fuego (Tipo de Riesgo –Medio).

TRD. 322.1.28.126

La entidad, a pesar de que cuenta con sistemas de protección, contra incendios, como son, extintores manuales, “conexiones alternas de energía” (en algunas áreas), equipos de bajo consumo, vías de acceso y de evacuación, amplias, etc., sin embargo, algún incidente involuntario, puede ocasionar, el inicio de un Incendio para lo cual se deberá proceder de la siguiente manera:

1. Si el inicio del incendio se produce en horas de labores, deberá de proceder a dar la alarma a todo el personal de la oficina, colindantes, 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 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).

4. Se deberá proceder a sofocar el fuego utilizando el extintor correcto para el tipo de fuego.

4) Aspecto de Seguridad en las Redes

3. Control de Acceso Físico a las Salas de Cómputo:

    1. Solo personal autorizado deberá ingresar a las áreas restringidas donde se encuentra la Sala de Servidores y/o otros lugares donde se encuentren los equipos informáticos; si otras personan ingresan debe ser con autorización y coordinación de la jefatura inmediata y en los tiempos establecidos y/o coordinados.

    2. Se recomienda contar con cámaras de seguridad en las áreas consideradas clave y en caso no se encuentre personal en una de esas áreas deberá estar cerrado por motivos de seguridad; y si dicha persona que está a cargo de las llaves se tendría que ausentar por un tiempo considerable, darle a otra persona a fin que se encargará de velar por el mismo.

    3. Adicionalmente también se deberían contar con detectores de humo, de calor que me indiquen cualquier cambio en los ambientes respectivos ya sea sala de servidores, centro de cómputo, etc. y me permitan posteriormente tomar las medidas necesarias.

4. Control de Acceso a la Red Vía PC.

    1. Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves o bloqueos de las PC.

    2. Solicitar clave de ingreso a la red y a los sistemas que están en red.

    3. Registrar toda la actividad de la estación de trabajo con el visor de sucesos.

    4. Retirar o inutilizar las disqueteras o unidades de almacenamiento, las PCs y/o Servidores donde se tenga información muy importante que ponga en riesgo la seguridad de la institución.

✓ Protección del Servidor

La parte más importante de la red lo conforman los servidores. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades. Los controles necesarios serían:

TRD. 322.1.28.126

1. 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.

2. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él.

3. Dada la importancia del servidor y la cantidad de datos que almacenan en él, es necesario efectuar copias de seguridad de los archivos y aplicaciones como configuraciones del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias para su correcto funcionamiento.

4. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

5. El área donde se encuentran los servidores debe estar con la suficiente 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.

11. ANÁLISIS DE RIESGOS

Para realizar un análisis de los riesgos, se procede a identificar y evaluar los objetos que deben ser protegidos, los daños que éste pueda sufrir, sus posibles fuentes de daño, su impacto dentro de la entidad y su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de éstos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

A. Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

- ✓ Personal.
- ✓ Hardware.
- ✓ Software y Utilitarios.
- ✓ Datos e información.
- ✓ Documentación.
- ✓ Suministro de energía eléctrica.
- ✓ Suministro de telecomunicaciones.

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o por causas humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese, por ejemplo: Cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

TRD. 322.1.28.126

c) Divulgación de información y que afecte su patrimonio estratégico y/o Institucional, sea mediante Robo o Infidencia.

B. Prioridades:

La estimación de los daños en los bienes y su impacto, fija una prioridad con relación a la cantidad de tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en dicho acontecimiento. Por lo tanto, los bienes que tienen más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

C. Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la institución son:

a) Acceso no autorizado

- ✓ Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
- ✓ Ruptura de las claves de acceso a los sistemas computacionales.
- ✓ Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (virus, sabotaje, ejecución de scripts malintencionados)
- ✓ Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

b) Desastres Naturales:

- ✓ Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de y/o de operación (equipos computacionales y/o servidores).
- ✓ Por fallas causadas por la agresividad del ambiente
- ✓ Inundaciones causadas por falla en los suministros de agua.

c) Fallas de Hardware y Equipos de Soporte.

- ✓ Falla en el Servidor de Aplicaciones, Servidor Proxy, Servidor Controlador Dominio y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.
- ✓ Falla en los Switches.
- ✓ Falla en el Cableado de la Red.
- ✓ Falla en el Firewall.
- ✓ Falla en el Aire Acondicionado en la Sala de Servidores.
- ✓ Incendios.
- ✓ Por fallas de red de energía eléctrica pública por diferentes razones ajenas.
- ✓ Por fallas de la comunicación.
- ✓ Por fallas en el tendido físico de la red local.
- ✓ Por fallas en las telecomunicaciones con instalaciones externas.
- ✓ Por fallas de Central Telefónica.
- ✓ Por fallas de líneas de fax.

d) Por fallas de Personal Clave.

Se considera personal clave aquel que cumpla una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información:

TRD. 322.1.28.126

a) Personal de Informática, Unidad Informática, supervisores de Red. Pudiendo existir los siguientes inconvenientes: Enfermedad, accidentes, renuncias, abandono de sus puestos de trabajo, otros imponderables.

D. Expectativa Anual de Daños

Para las pérdidas de información, se deben tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha sea menor o igual al necesario para la reposición del equipamiento que lo soporta.

E. Medidas Preventivas:

- Control de Accesos

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

- ✓ Acceso físico de personas no autorizadas.
- ✓ Acceso a la Red de PC's y Servidor.
- ✓ Acceso restringido a las librerías, programas, datos, logs de auditoria, etc.

- Previsión de desastres Naturales:

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Cómputo y/o servidores correspondientes en la medida de no dejar objetos en una posición tal que ante un movimiento telúrico de cierta magnitud pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, CD, discos externos, discos con información vital de respaldo de aquellos que se encuentren aún en las instalaciones. Se deberán tener el respaldo en lugares diferentes y con un código de identificación que maneje el personal de sistemas

- Adecuado Soporte de Utilitarios

La falla de los equipos deberá minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos a:

- ✓ UPS de respaldo de actual servidor de Red o de estaciones críticas.
- ✓ UPS de respaldo switches y/o HUB's.
- ✓ PCs en stock ante cualquier eventualidad que pudiera suceder.

- Seguridad Física del Personal

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 de los software y elementos de soporte relevantes, así como de documentar las incidencias y tener un registro de sus proyectos realizados y plan de trabajo. Estas acciones permitirán mejorar los niveles de

TRD. 322.1.28.126

seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

- Seguridad de la Información

La información y programas de los Sistemas de Información que se encuentran en el servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

12. PLAN DE RESPALDO

a) Objetivo:

Establecer un procedimiento para la administración de las copias de respaldos de información de los diferentes Sistemas de Información que se encuentran en producción y de los servicios de red de la organización. El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de sistemas, proyectos o ambientes, tendrán sus propios Planes de Respaldo.

b) Respaldo de datos Vitales Identificar las áreas para realizar respaldos:

a) Sistemas en Red.
b) Sistemas no conectados a Red.
c) Sitio WEB.
d) Correos electrónicos institucionales

c) Alcance.

Este procedimiento es aplicable a todos los sistemas de información en producción y los servicios de red de la organización.

d) Análisis de la Criticidad.

Primeramente, se deberá establecer la criticidad de los Sistemas de Información y los Servicios de Red de acuerdo al tipo de información que procesan y almacenan. Esta tarea deberá ser realizada conjuntamente por Soporte técnico y Administración de Sistemas. Esta tarea deberá ser realizada periódicamente, con el objetivo de revisar la criticidad, al menos dos veces por año o por demanda cuando se pone en producción un nuevo sistema de información o servicio de red y éste debe ser incluido en el plan de respaldos. Este análisis deberá estar enmarcado en los siguientes niveles de criticidad:

- ✓ Alta: El sistema y/o servicio posee información altamente crítica.
- ✓ Media: El sistema y/o servicio posee información medianamente crítica.
- ✓ Baja: El sistema y/o servicio posee información que no es crítica.

e) Toda la Información No es Crítica.

TRD. 322.1.28.126

Normalmente cuando uno plantea que va a respaldar los datos de su PC a una persona en una compañía y le pregunta que es crítico respaldar, casi siempre la respuesta es todo. Pero en realidad esto no es así, uno tiene que definir muy bien cuál es la información crítica, por ejemplo, la música que guarde un empleado en su PC no es crítica para las actividades de la empresa. En cambio, su correo electrónico, proyectos, informes y papeles administrativos si lo suelen ser y tener un respaldo de estos es clave para el funcionamiento de la empresa en caso de cualquier eventualidad. Lo importante de este punto es que NO TODA LA INFORMACIÓN ESCRÍTICA y hay que hacer un levantamiento de la que realmente lo es.

Otro punto importante es que dentro de la información crítica hay varios niveles, no es lo mismo perder los correos de un empleado que perder la información de nómina o de pago de los proveedores y siempre es aconsejable darle niveles de prioridad a la información para tener un mejor manejo de ella. Una vez que definamos que información realmente necesitamos respaldar vamos en buen camino y podemos seguir con nuestra política de respaldo. Normalmente la data o información que es respaldada por las empresas es: Archivos creados por aplicaciones, como por ejemplo .doc, .odt, .xls, .mdb, .pdf, .ppt entre otros.

- ✓ Archivos de correo electrónico
- ✓ Directorios telefónicos y de contactos
- ✓ Favoritos de los navegadores como Firefox e Internet Explorer
- ✓ Base de datos
- ✓ Configuraciones de los equipos
- ✓ Archivos de CAD, PSD, XCF, etc.
- ✓ Imágenes y Fotografías de proyectos
- ✓ Configuraciones de servicios
- ✓ Sistemas de la empresa

f) Plan de Respaldo y Responsables

El plan de respaldos contiene información de que sistemas de información y servicios de red serán respaldados, por lo que su periodicidad, tipo de respaldo, etc., estará determinado por la criticidad del sistema de información y/o servicio de red. Por otro lado, se realizarán las tareas de obtención de respaldos tomado en cuenta los horarios en los que el tráfico de datos de la red sea bajo; es decir, cuando no represente una carga excesiva en la red ni represente un trabajo adicional para los servidores de red cuando están trabajando los usuarios (ingresando, operando, realizando transacciones, etc.), por lo que los horarios correctos serán en horas nocturnas donde el tráfico de información es bajo.

El cronograma deberá contemplar claramente los siguientes campos:

- ✓ Responsable/s: Persona/s quien/es realizo/aron el plan.
- ✓ Fecha del plan: La fecha en la cual entra en vigencia el plan.
- ✓ Numero de plan: El número del plan, ejemplo: 001/2012
- ✓ Operador de Respaldos: Nombre y cargo de la persona que asume el rol.
- ✓ Revisor de Respaldos: Nombre y cargo de la persona que asume el rol.

g) Términos Usados.

- ✓ **Nivel de criticidad**: Nivel con la cual se ha establecido la criticidad, este puede ser:

a. Alta: El sistema y/o servicio posee información altamente crítica, por lo que debe ser respaldada al menos de forma diaria y una vez al mes.

b. Media: El sistema y/o servicio posee información medianamente crítica, por lo que debe ser respaldada al menos una vez por semana y una vez al mes.
c. Baja: El sistema y/o servicio posee información que no es crítica y por lo que debe ser respaldada al menos una vez por mes.

✓ **Periodicidad:** Es la frecuencia con la que se deberán realizar los respaldos, esta puede ser:

1. Diario: Realización de la copia de respaldo diariamente a disco duro.
2. Semanal: Realización de la copia de respaldo semanalmente a disco duro.
3. Mensual: Realización de la copia de respaldo mensual a cinta con las copias diarias y semanales acumuladas (HISTÓRICO).
4. A requerimiento: Realización de la copia de respaldo a requerimiento por una sola vez o por un tiempo determinado y puede ser temporal-diario o temporal mensual normalmente a requerimiento especial, a menudo usado para ambientes de prueba.

✓ **Tipo: Se refiere al tipo de respaldo.**

1. Total (Full): Es un respaldo completo de toda la información y configuración.
2. Diferencial (incremental): Es un respaldo de solamente la nueva información comparada con la información que posee el respaldo previo, por lo general a partir de un backup total.
3. Nombre de la tarea: El nombre de la tarea que se ejecutara para obtener el respectivo respaldo.

✓ **Responsables:**

El principal responsable es la persona que posee el rol de operador de Respaldos (backup operator) o se puede definir otro responsable exclusivamente en casos muy excepcionales.

✓ **Horarios:**

Los horarios se establecerán con el cuidado de no sobrecargar la red y los servidores, normalmente por las noches cuando la carga de interconexión y de procesamiento es muy baja.

✓ **Sitio:**

Lugar donde se encuentra el sistema de información y/o servicio de red en producción.

✓ **Medio:**

Medio en el cual se obtienen las copias de respaldo (Cintas, Dvds, etc.), número de copias: Se establecerá el número de copias, normalmente es de una copia de respaldo, pero puede establecerse más copias en algún caso especial (campo opcional).

h) Designación de Responsables

Se deberá designar formalmente a las personas responsables de la obtención de copias de respaldo, es decir, establecer la persona quien tendrá el rol de Operador de Respaldos, así como también el rol de Revisor de Respaldos, ambos roles se describen a continuación:

✓ **Respaldo Local:**

El respaldo local puede hacerse de varias formas en varios tipos de dispositivos. Los más comunes son:

1. Servidor de respaldo, con un arreglo RAID (múltiples discos en espejo), este servidor se coloca en red con una aplicación que respalde los datos automáticamente cada cierto tiempo, en estos tiempos el almacenamiento en disco duros es bastante económico y no se necesita que el servidor tenga una gran cantidad de recursos para efectuar esta tarea, casi siempre algún servidor que se haya sacado de circulación o inclusive una PC "vieja" puede hacer el trabajo. Claro hay servidores de alto desempeño para este tipo de tareas y la decisión va a depender del presupuesto con que cuenten.

2. Disco duro Externo en Red o USB, si la entidad no tiene presupuesto para un servidor y no cuenta con muchas estaciones de trabajo, un disco duro en Red o USB puede hacer las veces de sistema de respaldo, estos discos duros no suelen ser muy costosos y hay de todas las capacidades, lo ideal sería tener dos de estos en espejo en caso de que alguno falle. En caso de ser un disco duro USB se tiene que compartir en Red entre las PC de la empresa.

3. CDs, DVDs, si el respaldo que va a realizar no es tan periódico (1 o 2 veces al mes) puede utilizar un medio como un CD o DVD, en este caso sólo necesita una unidad capaz de grabar en cualquiera de estos medios y hay varias aplicaciones que permiten hacer el respaldo sin ningún problema. Si quiere utilizar el DVD o CD más de una vez se recomienda comprar los que son regrabables. Estos medios no suelen estar recomendados para respaldos muy periódicos, y casi siempre se utilizan para guardar información histórica de la empresa (como facturas, recibos, proyectos antiguos, etc).

   Además, se tiene que tener en consideración el almacenamiento seguro de estos discos en un contenedor cerrado que sólo tengan acceso personas autorizadas y que esté lejos del sol y la humedad. También se tiene que tener un sistema para catalogar y etiquetar que sea eficiente.

4. Cintas Magnéticas, este fue el sistema de respaldo preferido por muchos y aún muchas empresas lo utilizan, ahora son un poco difícil de conseguir además que su capacidad de almacenamiento es un poco limitada. Al igual que con los CDs y DVDs hay que tomar en cuenta el almacenamiento (lejos de campos magnéticos), etiquetado correcto y la rotación (de la que hablaremos más adelante) y además son medios que son reutilizables.

5. Se puede utilizar también una combinación de cualquiera de los métodos que planteamos. Por ejemplo, el respaldo del día a día se puede realizar en un servidor o disco duro externo y los históricos con más de un año de antigüedad en CDs y DVDs. Las desventajas de utilizar un medio de respaldo local es que en caso de desastre o robo se verán igual de afectados que nuestros demás equipos, normalmente la información más crítica se respalda en un medio como un DVD y se puede guardar en una caja fuerte si se tiene alguna en la empresa de esta manera si hay algún incendio o inundación no se verá afectada y tiene menos probabilidades de que sea robada. Aun así, el respaldo local es una medida muy importante y es la primera línea de defensa para salvaguardar la información de nuestra empresa.

- ✓ **Respaldo Remoto**

El respaldo remoto nos ayuda a protegernos contra desastres como incendios e inundaciones, contra robos y otras eventualidades que puedan ocurrir en el sitio principal de nuestra empresa. Este tipo de respaldo se puede realizar de varias formas:

TRD. 322.1.28.126

a) Servidor de Respaldos remotos, si nuestra empresa tiene varias sedes separadas geográficamente podemos colocar uno o varios servidores distribuidos entre las sedes para respaldar nuestra información a través de la red con una conexión segura. Así si pasa una eventualidad en alguna de nuestras sedes podemos recuperar la información fácilmente.

b) Servicios de Respaldo remoto, hay varias empresas que ofrecen el alquiler de servidores dedicados o servicios de respaldos, con este tipo de servicios no se necesitan tener varias sedes, simplemente se alquila el espacio que necesitemos para nuestro respaldo y se puede ir ampliando a medida que se necesite más. Este es uno de los servicios más populares de los que son llamados servicios de Nube donde una empresa ofrece capacidad y sistemas en demanda (on-demand) en la red. Asegurarse que a la hora de alquilar uno de estos servicios que tenga una fuerte política de seguridad y privacidad y que garanticen la integridad de sus datos, los proveedores de estos servicios están en la obligación de tener ciertas garantías de sus datos y de explicar cuáles son los mecanismos que utilizan para garantizarlos, si se rehúsan a explicar esto no confíe en el proveedor.

c) Estos dos son los principales métodos, también hay otra forma que es la de guardar los respaldos realizados en CDs y DVDs en otra localidad, igualmente que en el respaldo local de estos discos es importante un almacenamiento y etiquetado adecuado.

d) El respaldo remoto trae como ventaja la distancia geográfica que disminuye el riesgo de perder los datos, como desventaja tenemos que si se llega a perder la comunicación por períodos largos de tiempo no se puede realizar el respaldo con regularidad. La mejor solución es utilizar un respaldo local y remoto, así se tienen las ventajas de ambos y se compensan las desventajas de uno con el otro.

e) Como lo mencionamos anteriormente la información que sea más crítica y con mayor prioridad se puede respaldar en ambos sistemas mientras que la menos crítica se puede hacer solamente local, lo cual disminuye los costos de inversión.

i) Uso de los Respaldos Se establecen dos situaciones:

- ✓ **Uso para propósitos de revisión:** Los medios antes de ser enviados al custodio, la persona con el rol de Revisor de Copias de Respaldo, podrá solicitar el medio, al Operador de Copias de Respaldo, cuando así lo considere (aleatoriamente) para restaurar en otro ambiente que no sea el de producción, con propósitos de revisión y control y poder certificar el proceso de obtención de **copias de respaldo.**

1. **Uso para restablecer los Sistemas de Información y/o los Servicios de Red:** Para la obtención y utilización de los medios donde se encuentra información de respaldo y con el propósito de restaurar los mismos ante posibles incidentes (Administración de Problemas e Incidentes, Administración del Plan de Contingencias, etc.), solo podrán ser solicitados por el responsable de las copias de seguridad y con la aprobación del Jefe de Área correspondiente.

j) Análisis de Impacto de los Procesos

a) Objetivo Principal:

El objetivo principal del Análisis del Impacto de los procesos, es determinar las funciones, procesos e infraestructura de soporte que son críticos para la contingencia operativa de la entidad.

TRD. 322.1.28.126

b) Objetivos Específicos:

Para lograr el objetivo principal se definieron los siguientes objetivos específicos:

2. Identificar las preocupaciones y prioridades de la Alta Dirección en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.

3. Identificar el tiempo máximo en el que un proceso crítico de la entidad deberá ser restaurado para su normal y eficiente continuidad.
4. Identificar el impacto en las aplicaciones que soportan los procesos críticos de la entidad.
5. Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

k) Sistemas de Información del Hospital

Los principales sistemas existentes en el Hospital son:

- ✓ Dinámica Gerencial.
- ✓ Cnt
- ✓ Caduceos
- ✓ Ant-wimax.

l) Principales servicios que deberán ser restablecidos Y/O recuperados (Centro de Cómputo Alterno)

- ✓ **Generales**

a. Windows
b. Correo Electrónico
c. Internet.
d. Antivirus.
e. Herramientas de Microsoft Office.
f. página web.

- ✓ **Software Base**

a. Base de Datos Sql
b. Backup de la Información.
c. Ejecutables de las aplicaciones.

- ✓ **Respaldo de la Información**

a. Backup de la Base de Datos Sql
b. Backup de la Plataforma de Aplicaciones (Sistemas)
c. Backup de la WEBSITE
d. Backup del Servidor controlador de Dominio.
e. Backup del Servidor de Archivos.

13. PLAN DE RECUPERACION

a. Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

TRD. 322.1.28.126

f) Determinación de las políticas y procedimientos para respaldar las aplicaciones y/o los datos.
g) Planificar la reactivación dentro de las 5 horas como máximo de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
h) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
i) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.
j) Restablecer en el menor tiempo posible el nivel de operación normal del Centro de Procesamiento de la información y/o de los Servidores correspondientes, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputo y de los demás niveles.

b) Lista de Verificación

Para Un Plan de Recuperación de Desastres Cuando hablamos de ejecutar una Recuperación de Desastres de nuestra red o de la Continuidad del Negocio, el tiempo y la precisión son de alta importancia. Las metas de una recuperación de desastres y la continuidad del negocio son sensitivas en el tiempo y bastante críticos, por lo que el uso de una Lista de Verificación se convierte en una herramienta ideal cuando nos afrontamos a una situación en donde esos planes son requeridos.

Las siguientes actividades definen una seria de acciones o actividades que deben entrar en juego cuando se requiere ejecutar una recuperación de desastres:

1. Detectar una falla y efectos de desastres lo más rápido posible.
2. Notificar a los responsables que deben tomar acción.
3. Aislar los sistemas afectados para limitar el alcance de las fallas y daños.
4. Reparar o reemplazar sistemas críticos, y trabajar hacia una continuidad en las operaciones normales, si es que las circunstancias lo permiten.

El Plan de Recuperación viene de la mano del Plan de Respaldo, pues de la información respaldada se realiza la recuperación en caso de algún inconveniente. La restauración de los datos es el fin por el que hay que luchar a la hora de realizar una buena planificación de copias de seguridad. Los Backus tienen como objetivo hacer frente a cualquier pérdida de datos y poder mantener la continuidad del negocio, por lo que, si contamos con una correcta planificación de copias de seguridad, lo único que nos falta para que la organización pueda seguir funcionando es restaurar los datos y volver a la situación previa al desastre o la interrupción en lo que respecta a los sistemas de información.

c) Alcance del plan de recuperación.

La responsabilidad sobre el Plan de Recuperación es de la Unidad de Administración y el Personal de Sistemas con una persona encargada de ejecutarlo, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

La duración del plan se determinará de acuerdo a las necesidades que se presenten y la capacidad de los equipos de trabajo para procesar la restauración y recuperación de los sistemas. De igual forma se puede crear un comité entre el mismo personal que tenga conocimientos suficientes para determinar si la recuperación puede realizarse con todas las condiciones favorables.

d) Activación del Plan:

TRD. 322.1.28.126

La decisión queda a juicio de la oficina de Gestión de la Información, determinando la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

e) Duración estimada

Los supervisores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

f) Responsabilidades

- Orden de Ejecución del Plan: Gestión de la Información
- Supervisión General de Plan: Propia de la oficina Gestión de la Información
- Supervisión del Plan de Recuperación: Lideres de procesos.
- Abastecimiento (HW, SW): Técnico de sistemas.
- Tareas de Recuperación: Personal de tareas afines.

g) Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables).

h) Priorizar el Recupero de Recursos.

Listar la prioridad asociada con el recupero de un recurso específico, basado en la caída del impacto y el tiempo de caída aceptable. Usar escalas cuantitativas o cualitativas Alto, Medio, Bajo).

Priorizar el recupero de Recursos.

RECURSOS	PRIORIDAD DEL RECURSO
pc	ALTO
Impresora	ALTO
Servidor base de datos	ALTO
Servidor de archivos	ALTO
Servidor de control de dominios	ALTO
Internet	ALTO
Servidor de correos	ALTO
Página web	ALTO
Herramientas de office	MEDIO

Asegurar que la estrategia elegida pueda implementarse de manera eficaz con el Personal y recursos financieros disponibles y se ejecute de manera correcta la continuidad de los procesos y servicios de

TRD. 322.1.28.126

la entidad. Se debe determinar un presupuesto de gastos para el planeamiento de contingencias referente a:

- ✓ Software y hardware.
- ✓ Transporte.
- ✓ Pruebas.
- ✓ Entrenamiento.
- ✓ Materiales.
- ✓ Tiempo a incurrir.
- ✓ Servicios, etc.

i) Detalla algunas de las causas de la Falla del Servidor.

CASO A: Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y enviar correos a los líderes del área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

1. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

2.Ante procesos mayores se congela el proceso.

3. Arroja errores con mapas de direcciones hexadecimales. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

a) Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y telefonear a los jefes de área.

b) El servidor debe estar apagado, dando un correcto apagado del sistema

c) Ubicar las memorias malogradas.

d) Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.

e) Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

f) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el

TRD. 322.1.28.126

concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

g) Probar los sistemas que están en red en diferentes estaciones.

h) Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

1. Caída del servidor de archivos por falla de software de red.

2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

3. Bajar incorrectamente el servidor de archivos.

4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

- Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos; una vez mostrado el prompt de DOS, cargar el sistema operativo de red.

- Deshabilitar el ingreso de usuarios al sistema.

- Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

- Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

- Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que los índices en la base de datos estén correctos, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente. Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

j) Consecuencias de la Interrupción del Fluido Eléctrico

A continuación, se presenta una tabla donde se listan las consecuencias de interrupción de fluido eléctrico

CONSECUENCIA/IMPACTO	AREAS AFECTADAS
Cierre Inapropiado de la Base de Datos	Todas las áreas
Finalización Incompleta de los Backups	Todas las áreas
Finalización Incompleta de los Backups	Todas las áreas
Pérdida total o parcial de la operatividad de los sistemas	Todas las áreas

TRD. 322.1.28.126

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.

2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.

3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados a corriente normal (o UPS) donde:

Corriente de emergencia, a la brindada por UPS.

Corriente normal, a la brindada por la empresa de energía eléctrica.

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores con motores de base de datos de Sql, por tal motivo es necesario revisar continuamente el estado de las baterías del UPS.

Dichas baterías deben garantizar una autonomía de aproximadamente una hora. Es necesario establecer un procedimiento que permita al personal de seguridad de la entidad avisar al personal de Informática de este hecho. El UPS se caracteriza por emitir una alarma fácil de identificar.

k) Recursos de Contingencia Generales

Se debe tener recursos de contingencia tales como:

- Router (Proveído por el proveedor de Internet y WAN).
- Tarjeta de Red,Conector RJ45,Jack RJ-45,Testeador.
- Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).
- Gabinete de Comunicaciones y Servidores.
- Materiales Y herramientas para cableado Estructurado.
- UPS y Equipos de aire acondicionado.
- Backup diario de la información de los Sistemas.
- Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.
- Componente de Remplazo (Memoria, Disco Duro, UPS, etc.).
- Si existiere problema en las antenas, puede ser por problema de posición al direccionar las antenas, se recomienda mover las antenas y ver si el equipo se reestablece, en caso extremo contar con un Servidor Vpn que haga de respaldo hasta que se solucione el inconventiente.

l) Impacto de la Caída y tiempos Aceptables de Caida

A continuación, se muestra la tabla de impactos y tiempos de caída aceptables:

RECURSO/SERVICIO	IMPACTO	TIEMPO ACEPTABLE DE CAIDA

TRD. 322.1.28.126

Servidor de Base de Datos	Alto	1 hora
Servidor de Aplicaciones	Alto	1 hora
Servidor controlador Dominio	Alto	1 hora
Servidor de Archivos (acceso a los documentos)	Alto	2 horas
Internet	Alto/Medio	1 hora
Página web	Alto/medio	1 hora

m) Contenido del plan de contingencia para la Coordinación Administrativa de Tecnologías de Información:

- Listas de notificación, números de teléfono, mapas y direcciones.
- Prioridades, responsabilidades, relaciones y procedimientos.
- información sobre adquisiciones y compras
- Diagramas de las instalaciones
- Sistemas, configuraciones y copias de seguridad en cinta o cualquier otro medio.
- Medios de comunicación como radios, celulares ante cualquier incidencia.

n) Procedimientos para las Pruebas del Plan de Contingencias - Niveles de Prueba Se recomiendan dos niveles de prueba:

- Pruebas en pequeñas Unidades funcionales.
- Pruebas en a nivel Gerencial. La premisa es comenzar la prueba en las Unidades funcionales más pequeñas, extendiendo el alcance a nivel Gerencial, para finalmente realizar las pruebas entre sedes o con otras instituciones externas.

o) Métodos para Realizar Pruebas de Planes de Contingencia

✓ **Prueba Específica**

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

✓ **Prueba de Escritorio**

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios). Las características de la prueba de escritorio son:

- ✓ La discusión se basa en un formato preestablecido.
- ✓ Está dirigido al equipo de recuperación de contingencias.
- ✓ Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad.

Los ejercicios de escritorio son ejecutados por el encargado de la prueba y el personal responsable de poner el Plan de Contingencia en ejecución, en una situación hipotética de contingencia de preguntas se pedirá que resuelva el personal.

El encargado y el personal utilizarán el Plan de Contingencia para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios

TRD. 322.1.28.126

están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

- ✓ **Simulación en Tiempo Real**

Las pruebas de simulación real, en una Unidad, áreas en la entidad están dirigido a una situación de contingencia por un período de tiempo definido.

1. Las pruebas se hacen en tiempo real.
2. Son usadas para probar partes específicas del plan.
3. Permiten probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

p) Preparaciones PRE Prueba

1. Repasar el plan de contingencia.

2. Verificar si se han asignado las respectivas responsabilidades.

3. Verificar que el plan este aprobado por la dirección de la entidad.

4. Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.

5. Establecer la fecha y hora para la ejecución de la prueba.

6. Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.

7. Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.

8. No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.

9. La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.

10. Enfocar los procesos críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.

11. Definir el ambiente donde se realizarán las reuniones del equipo de recuperación de contingencias.

12. Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

q) Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

Si es necesario, el hardware y software necesarios deben activarse o adquirirse, así como ser transportados al sitio alterno; las estrategias básicas para disponer de equipo de reemplazo son:

TRD. 322.1.28.126

(1) Acuerdos con proveedores:

Se establecen acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.

(2) Inventario de equipos: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa (el sitio alterno).

(3) Equipo Compatible Existente:

(a) Equipo existente en sitios alternativos.
(b) Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación.
(c) Almacenar un equipo sin usar es costoso, pero permite que la recuperación comience más rápidamente.
(d) Considerar la posibilidad de un desastre extendido que requiere reemplazos masivos de equipos y retrasos del transporte.
(e) Mantener listas detalladas de necesidades de equipo y especificaciones dentro del Plan de Contingencia.
(4) Infraestructura del Ambiente Alterno PROPIO:
Para este escenario, se requiere condicionar un ambiente alterno que pueda ser utilizado como sala de servidores en el momento de la contingencia con las dimensiones apropiadas para facilitar la ubicación de los equipos y mobiliario. El ambiente alterno contaría con los siguientes recursos:

(a) 3 mesas para monitores y teclados de los servidores principales
(b) 2 sillas
(c) Switches 24 Ports (10/100/1000)
(d) 1 Router para la conexión a internet
(e) 1 UPS
(f) 1 Teléfono
(g) 1 Extinguidor Clase A (Gas Carbónico)
(h) Útiles de Oficina

14. PLAN DE MANTENIMIENTO

En la mayoría de las organizaciones los cambios ocurren todo el tiempo. Los productos y los servicios cambian continuamente en todos los niveles. El aumento de procesos basados en tecnología, ha incrementado significativamente el nivel general de dependencia sobre la disponibilidad de sistemas e información para que la entidad opere efectivamente. Es por lo tanto necesario que el Plan de Contingencia, se adecue a esos cambios y se mantenga continuamente actualizado.

Cuando se realizan cambios al Plan de Contingencia se deben probar completamente y hacer las correcciones requeridas. Esto implica el uso de procedimientos formales de control de cambios bajo el manejo de la persona encargada del equipo del Plan de Contingencia.

1. Control de cambios al Plan de Contingencia.
2. Responsabilidad en el mantenimiento de cada parte del plan.
3. Pruebas a todos los cambios del plan.
4. Aviso a persona responsable del mantenimiento.

TRD. 322.1.28.126

A. Control de Cambios al Plan

Se recomienda establecer controles formales del cambio para cubrir cualquier modificación que se tenga al Plan de Contingencia. Esto es necesario debido al nivel de complejidad contenida dentro del plan. Se debe preparar una plantilla para solicitud de cambios y debe ser aprobada previamente.

B. Responsabilidad en el Mantenimiento de Cada Parte del Plan

Cada parte del plan será asignada a un miembro del equipo del Plan de Contingencia o un Supervisor de la entidad, que será responsable de actualizar y mantener el plan. La persona encargada del equipo de Plan de Contingencia, mantendrá el control completo del Plan de Contingencia, pero los jefes de las unidades necesitarán mantener sus propias secciones al día.

C. Pruebas a todos los cambios del Plan

El equipo del Plan de Contingencia, nombrará una o más personas que serán responsables de coordinar todos los procesos de prueba y asegurar que todo cambio al plan se prueba apropiadamente. Cuando los cambios se hacen o son propuestos al Plan de Contingencia, se debe notificar al coordinador de pruebas del Plan de Contingencia. Se deberá probar los procedimientos de cambio para asegurar la calidad de los mismos. Esta sección del Plan de Contingencia, contiene una comunicación del coordinador del Plan de Contingencia a las unidades de la entidad afectadas y contiene información acerca de los cambios que se requieren probar o reexaminar.

15. PLAN DE ENTRENAMIENTO

Todo el personal del Área de Informática, debe entrenarse en el proceso de Recuperación del Plan de Contingencia. Esto es particularmente importante cuando los procedimientos son significativamente diferentes de las operaciones normales y se requiere un desempeño excelente para garantizar la restauración de los equipos de cómputo.

La capacitación se debe planear detenidamente y debe ser completamente estructurada y coherente acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.

- ✓ Objetivos del Entrenamiento:

a. Entrenar todo el personal en los procedimientos particulares a seguir durante el proceso de recuperación del Plan de Contingencia.

b. Difusión del Plan de Entrenamiento.

- ✓ Alcance del Entrenamiento

a. La capacitación se llevará a cabo de manera exhaustiva para que se llegue a estar familiarizado con todos los aspectos del proceso de recuperación.

b. La capacitación cubrirá todos aspectos de la sección de actividades de recuperación del Plan de Contingencia.

c. Es importante desarrollar un programa institucional que cubra las partes esenciales requeridas para comunicar los procedimientos del proceso de recuperación de negocio de la entidad.

TRD. 322.1.28.126

- ✓ Revisión y Actualización El seguimiento permanente permite conocer la evolución, los cambios en condiciones actuales, el cumplimiento de metas propuestas y los ajustes requeridos. La evaluación periódica del Plan de Contingencia se realiza a través de:

a. Simulacros
b. Simulaciones
c. Evaluación del desempeño por evento

- ✓ La simulación y simulacros

Las simulaciones y simulacros son evaluaciones muy importantes, pues entrenan al personal, enfrentándolo en situaciones probables de emergencia o desastres y ponen a prueba la capacidad de la entidad ante los riesgos que pudiera ocasionar. Los simulacros, llamados también ejercicios de evaluación, constituye la actividad práctica por excelencia en el proceso de preparación del Plan de Contingencia para situaciones ante desastres. Las simulaciones, son ejercicios de escritorio que se realizan en situaciones ficticias controladas.

- ✓ Guía para simulaciones y simulacros

a. Conformar un Comité de emergencia y defina sus funciones.
b. Evaluar los riesgos informáticos, y la vulnerabilidad de la entidad
c. Realizar un inventario de recursos humanos y materiales.
d. Elaborar un plan para la atención de del centro de cómputo y centro de cómputo alterno.
e. Difundir el plan a todo el personal de la entidad
f. Coordinar con las instituciones que nos prestan servicios y/o asociados.

Realizar simulaciones o ejercicios de escritorio.

- ✓ Evaluación del Simulacro

Todas las conclusiones deben integrase en un documento para uso del comité, con la finalidad de facilitar el proceso de ajuste del plan de acuerdo a los resultados. Los pasos son:

a. Reunión con las comisiones o brigadas de las áreas de la entidad.
b. Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
c. Difusión del documento de evaluación.

- ✓ Errores Frecuentes en la Realización de los Simulacros

a. Improvisación y falta de planificación adecuada al simulacro.
b. Falta de entrenamiento del personal participante en los procedimientos que se desarrollan.
c. Dificultares disciplinarias con los simuladores, que en ocasiones no asumen la ejecución de los ejercidos con la responsabilidad requerida.
d. Falta de coordinación entre las diferentes entidades involucradas participantes del simulacro.

- ✓ Comunicación al personal

Una vez se defina la capacitación a ser impartida al personal, es necesario avisarles acerca del programa de capacitación en el que se requiere su asistencia y saber si puede asistir en dichas fechas y horas señaladas. Se deberá enviar una comunicación separada a los jefes de Unidad y/o Area, encargados del hospital, avisándoles del horario propuesto de entrenamiento para que su personal asista.

TRD. 322.1.28.126

- ✓ Evaluación del entrenamiento

a. Se debe valorar el programa de capacitación individual del Plan de Contingencia y el Plan de Contingencia Completo, para asegurar su calidad, eficacia y aplicabilidad.
b. Esta información se tomará de los entrenadores y también de las personas que toman los entrenamientos. Este proceso se hará con cuestionarios al final, con el propósito de tener retroalimentación.

16. RESPONSABLES

Responsables de la elaboración del Plan:

Ing. Yanet moreno
Wilmar Lizcano
Leidy Katherine Mejia.

Responsable de Ejecución: Ing. Yanet moreno y Wilmar Lizcano.

17. ANEXOS

Procedimiento de Apagado y Encendido de Servidores.

1. Pasos a Seguir para el Encendido de Servidores:

a) Identificar el botón de encender el equipo servidor y presionar.
b) Si el servidor se encuentra encendido se ingresa a esta por medio del acceso remoto.
c) Ingresar el usuario y la contraseña del ADMINISTRADOR DE DOMINIO.
d) Identificar los servicios que se tienen que levantar para su correcto funcionamiento de las aplicaciones Instaladas (Usualmente está configurado el inicio automático de los servicios cuando inicia el sistema Operativo).

2. Lista de Personal de Equipo de Respuesta a Desastres.

Ante un desastre a la hora de ocurrir el problema estas son las personas críticas que deberán ubicar según el problema suscitado, para dar el apoyo ante la emergencia suscitada.

Respaldo de datos Vitales

Identificar las áreas para realizar respaldos:

- Sistemas en Red.
- Sistemas no conectados a Red.
- Sitio WEB.
- **Archivos.**

Plan de Contingencia en los Sistemas de Información ante los cortes de energía

Ante un posible corte de energía, se deberá realizar el registro manual de los documentos, posteriormente cuando se restablezca el servicio de la energía eléctrica se deberá regularizar los documentos para posteriormente tener los reportes adecuados. Para ello se deberá contar con formatos

TRD. 322.1.28.126

disponibles para tal caso. No regularizar la información en el sistema traerá como consecuencia tener reportes estadísticos y/o operativos incompletos, así como inconsistencias de información lo que hará que la toma de decisiones no sea la acertada.

Plan de Contingencia de los Equipos informáticos ante los cortes de energía

Como todo componente electrónico el computador puede sufrir desperfectos ante con un corte de electricidad, un aumento de energía o una baja, esto incluye cualquiera de sus partes como el disco duro, placa base, memorias, procesador, etc.

El hecho de que se tenga un regulador de voltaje no te salva del todo, el regulador te protege en un cierto porcentaje más no en todo, el conjunto es lo que hace la diferencia, por ejemplo: Un computador con un buen regulador de voltaje, pero con una fuente de poder baja o de mala calidad está más propenso a una muerte por un alza eléctrica que uno que tenga una buena fuente de poder. La placa también es importante, quizás el componente más importante. La tierra eléctrica es muy importante, sin este el regulador está ahí solo de adorno.

Con respecto al sistema si es factible que puedan fallar algunos programas y o archivos para lo cual se deberán contar con el backup de los instaladores correspondientes y últimos archivos, y así ejecutar programas de recuperación si el caso lo amerita. A menos que se tenga un notebook, cuando hay un corte de luz, tu PC se apagará y todo el trabajo que no se haya guardado se perderá. Pero, a veces, cuando restauran la energía eléctrica, la PC no vuelve a encender más porque se quemó la fuente.

¿Por qué se quema la fuente?

Cuando vuelve la luz, en el mejor de los casos, y por suerte el más frecuente, sólo se te quema la fuente. Esto sucede porque, cuando restauran la energía eléctrica, el voltaje que viene es un algo mayor a los 220V y los circuitos internos de la fuente no lo soportan y se queman. En el peor de los casos, puede suceder que parte de esa corriente llegue al motherboard, quemando varios de sus circuitos.

¿Cómo Protegerse?

Para protegerse de la sobre-carga de tensión eléctrica, se tiene dos opciones:

a) Estabilizador de tensión

La corriente eléctrica que nos proporcionan (Ej. Luz del sur), nunca tiene 220V o 110V constantes. Siempre tiene fluctuaciones en unos 2 o 3 voltios. Lo que este dispositivo hace, como dice su nombre, estabiliza la tensión de la corriente eléctrica. Recibe la tensión como viene y entrega SIEMPRE 220V o 110V constantes. Si tu PC está conectado a un estabilizador de tensión, siempre va a recibir 110V, ni más ni menos.

Aunque tengas una baja de tensión, tu PC recibirá 110V.

- ✓ Ventajas:

a. Siempre entrega la tensión estabilizada.

b. Es económico.

TRD. 322.1.28.126

c. Necesita poco y nada de mantenimiento.

- ✓ Desventajas:

a. Si hay un corte de luz, tu PC se apaga.

b) UPS o Sistema de Energía Ininterrumpida

La UPS es como el estabilizador, con la diferencia de que tiene una batería, que provee de energía en caso de un corte de luz. La mayoría de las UPS, te entrega la energía estabilizada, como el estabilizador de tensión.

Cuando hay un corte de luz, cambia a modo de batería en unos pocos milisegundos, y comienza a entregar energía desde la batería. De este modo, puedes seguir trabajando unos minutos más, guardar tu trabajo y apagar correctamente la PC.

Algunas UPS, incluso traen un programa para que apague la PC, en caso de que haya un corte de luz cuando uno no se encuentra en la oficina. La batería te provee de energía por unos 10 a 15 minutos, suficiente para que guardes todo tu trabajo y apagues la PC.

- **Ventajas:**

- En caso de un corte de luz, puedes seguir trabajando unos minutos más.
- Te entrega siempre la corriente estabilizada.
- Algunas UPS vienen con un programa que te apaga la PC automáticamente.
- Necesita poco mantenimiento. Sólo necesitas drenar la batería cada 6 meses.

- **Desventajas**:
- Son más caras que los estabilizadores de tensión.
- Son bastante pesadas, debido a la batería. Igualmente, no es grave, ya que estarán en el piso y no la vas a estar moviendo de un lado a otro constantemente.

18. Conclusiones

El presente Plan de Contingencia, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información de la ESE, extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

Las principales actividades requeridas para la implementación del Plan de Contingencia son:

- Identificación de Riesgos,
- Evaluación de riesgos,
- Asignación de prioridades a las aplicaciones,
- Establecimiento de los requerimientos de recuperación,
- Elaboración de la documentación,
- Verificación e implementación del plan,
- Distribución y mantenimiento del plan.

El plan de Contingencia de la entidad está sujeto a la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Sala de Servidores. Lo único que realmente permitirá a entidad reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

19. Recomendaciones

Se enuncian las siguientes recomendaciones:

a) Programar las actividades propuestas en el presente Plan de Contingencias.

b) Hacer de conocimiento general el contenido del presente Plan de Contingencia, con la finalidad de instruir adecuadamente al personal de la entidad.

c) Adicionalmente al Plan de Contingencia se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

d) Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la entidad.

e) Autorizar el manejo de la información por perfiles y a los usuarios correspondientes. Dar niveles de acceso a la información.

f) Tener componentes de reserva y/o en stock para poder reemplazar los equipos en el momento adecuado, como componentes de servidor como discos duros, lectoras, switches, etc. que se puede necesitar ante cualquier eventualidad.

g) En el caso de las antenas que comunicaban sedes, si estas dejasen de funcionar es recomendable tener otra vía de comunicación como un enlace VPN, para ello se requiere un aceptable ancho de banda.

h) Hacer los backups correspondientes de información según prioridad como contingencia de eventos imprevistos que afectasen la información

1. CONTROL DE CAMBIOS.

REVISIÓN N°	FECHA DE APROBACIÓN DD/MM/AA	DESCRIPCIÓN DE CAMBIOS
01	2018-08-13	Creación del Documento

TRD. 322.1.28.126

	-	