M E M O R A N D O

Ref. GA-2017-11

PARA: **Licda. Verónica Villalta**
Directora Ejecutiva Fosalud

DE: **Benigno Andrés Mercado**
Gerente Administrativo

FONDO SOLIDARIO PARA LA SALUD Fosalud GERENCIA ADMINISTRATIVA EL SALVADOR, C.A.

ASUNTO: Solicitud aprobación del Plan de Contingencias 2017 para servicios informáticos proporcionados por la Unidad de Tecnologías de Información.

FECHA: **07 de Marzo de 2017.**

Estimada Licenciada Villalta, hago de su conocimiento que la Unidad de Tecnologías de información en base a requerimientos de la Auditoría TIC de la CCR ha elaborado el PLAN DE CONTINGENCIAS 2017 PARA SERVICIOS INFORMÁTICOS PROPORCIONADOS POR LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Comentarle, según Manual de Políticas y Procedimientos de la Unidad de Tecnologías de Información. Procedimiento 1, Políticas y procedimientos de Planeación y Gestión estratégica. Literal B, Procedimientos de Planeación Estratégica. Numera 3, relativo al Plan de Contingencias, el cual reza: Este documento deberá ser presentado a la Dirección Ejecutiva y Gerencia Administrativa para su aprobación.

Este **Plan de Contingencias** ha sido diseñado para ser el patrón de seguimiento de ante casos fortuitos y de fuerza mayor, al cual responderán los miembros de la Unidad de Tecnologías de Información del FOSALUD. Formará parte de este plan todos los seguimientos realizados al mismo por parte de los responsables, así como las actualizaciones y/o modificaciones realizados durante el año. Este documento estará vigente durante el año de su desarrollo y deberá ser revisado y/o actualizado cada año.

Sin otro particular, me suscribo de usted.

Atentamente,

FOSALUD
DIRECCION EJECUTIVA
RECEPCION DE CORRESPONDENCIA
HORA: 8:10 a.m.
FECHA: 07-03-17
FIRMA:

Fecha elaboración:	Responsable de elaboración: Ing. Nelson Eduardo Najarro Alvarez. Jefe de la Unidad de Tecnologías de Información Firma:
Revisión por la Gerencia Administrativa.	Responsable revisión: Ing. Benigno Andrés Mercado Gerente Administrativo Firma:
Aprobación por la Dirección Ejecutiva.	Responsable aprobación: Licenciada Verónica Villalta Directora Ejecutiva. Firma:

Según Manual de Políticas y Procedimientos de la Unidad de Tecnologías de Información. Procedimiento 1, Políticas y procedimientos de Planeación y Gestión estratégica. Literal B, Procedimientos de Planeación Estratégica. Numera 3, relativo al Plan de Contingencias, el cual reza: Este documento deberá ser presentado a la Dirección Ejecutiva y Gerencia Administrativa para su aprobación.

FONDO SOLIDARIO PARA LA SALUD

FOSALUD.

PLAN DE CONTIGENCIAS 2017 PARA SERVICIOS INFORMATICOS PROPORCIONADOS POR LA UNIDAD DE TECNOLOGIAS DE INFORMACION

San Salvador, 14 de febrero de 2017.

Gerencia Administrativa.

CONTENIDO.

INTRODUCCIÓN.

En cumplimiento al manual de políticas y procedimientos de la unidad de tecnologías de información. Procedimiento No. 1, Políticas y procedimientos de planeación y gestión estratégica. Literal A, Políticas de Planeación y Gestión Estratégica. Inciso No. 6, en su parte final, la cual reza **"Deberá establecer planes de contingencia, las cuales deberán revisarse anualmente".**

Este manual ha sido diseñado para ser el patrón de seguimiento de ante casos fortuitos y de fuerza mayor, al cual responderán los miembros de la Unidad de Tecnologías de Información del FOSALUD. Formará parte de este plan todos los seguimientos realizados al mismo por parte de los responsables, así como las actualizaciones y/o modificaciones realizados durante el año. Este documento estará vigente durante el año de su desarrollo y deberá ser revisado y/o actualizado cada año.

La jefatura de la Unidad de tecnologías y los responsables de las Secciones de dicha unidad deberán dar el debido seguimiento sobre la base de las responsabilidades asignadas en el cronograma. El cronograma de actividades brindara

OBJETIVOS DEL MANUAL.

1. Ser una guía al personal de la Unidad de Tecnologías, brindando los lineamientos específicos para mantener en operación los diferentes servicios prestados por la unidad.

2. Brindar la mayor eficiencia, calidad y control de las operaciones, ahorrando tiempos y esfuerzos en la ejecución de las actividades de restablecimiento de servicios, de forma que se eviten las duplicidades dentro de los procesos y se detallen claramente las responsabilidades.

3. Apoyar la reducción de riesgos que impactan en los procesos administrativos de la institución y los cuales son apoyados con medios tecnológicos responsabilidad de la unidad de tecnologías de información.

ALCANCE.

Deberán ser considerados como parte de este manual los procesos necesarios para recuperación de servicios electrónicos y/o mecanizados de índole informática, utilizados directamente por los usuarios.

RIESGOS DETECTADOS

El Plan Operativo 2017 de la unidad de tecnologías de información describe como riesgos potenciales los siguientes elementos:

- Desabastecimiento de suministros informáticos para la operación institucional.
- El servidor de aplicaciones opera con fallos, volviéndolas inaccesibles.
- Pérdida de dato de usuarios.
- No contar con la información para la elaboración de los indicadores en salud.
- Existen fallas en los servicios prestados al usuario.

N°	PROCESO	SUPUESTO	RIESGO POTENCIAL	PROBABILIDAD DE OCURRENCI	IMPACTO (1-5)	NIVEL DE RIESGO	ACCIONES	ACTIVIDADES PARA ELIMINAR O MITIGAR DEL RIESGO	IEDIOS DE VERIFICACIÓ	RESPONSABLE
P01UTI	Brindar soporte técnico a usuarios, mantenimiento, control y administración de activos informáticos y suministros.	Abastecimiento de suministros informáticos suficiente para la operación institucional.	Desabastecimiento de suministros informáticos para la operación institucional.	2	4	BAJO	Aceptar	Monitorear del consumo de suministros.	Informe de consumos de suministros.	Técnico de Activos y Soporte Tecnológico
P02UTI	Automatizar procesos	El servidor de aplicaciones opera sin fallos.	El servidor de aplicaciones opera con fallos, volviéndolas inaccesibles.	2	5	MODERADO	Monitorear	Monitorear respaldos de aplicaciones y bases de datos en servidor secundario.	Correos electronicos automaticos de respaldos realizados.	Enc. Sección DSAP
P03UTI	Gestionar portales de comunicación digital y administración de seguridad de la información	Mantener respaldo de Usuarios.	Perdida de dato de usuarios.	2	5	MODERADO	Monitorear	Realizar revisiones periódicas de sincronización de herramienta de respaldo de datos de los usuarios.	Reportes de Sincronización de herramienta de respaldos.	Encargados de Sección de Redes y Comunicaciones
P04UTI	Procesar información de producciones de establecimientos y acciones de personal.	Ingreso de datos en fechas y tiempos estipulados.	No contar con la información para la elaboración de los indicadores en salud.	2	5	MODERADO	Monitorear	Monitorear el volumen de producciones y redistribuir de manera equitativa el procesamiento de datos de las regiones.	Informes de procesamientos de datos de los sistemas de salud.	Encargada de registro de producciones y movimientos de personal
P05UTI	Gestión estratégica	Los servicios prestados al usuario funcionan correctamente.	Existen fallas en los servicios prestados al usuario.	2	5	MODERADO	Monitorear	Seguimiento del plan de contingencias de la unidad de tecnologia.	Documento de Plan contingencias y registros de seguimiento.	Jefe UTI

*Los riesgos de información y desabastecimientos de suministros se deberán seguir solo como parte del Plan del Operativo, ya que no forman parte de los alcances de este manual.

Sobre la base de estos riesgos se puede mencionar que es necesaria la creación de planes de acción para los siguientes procesos:

- Recuperación de las aplicaciones en producción.
- Procedimiento para la recuperación de datos de los usuarios.

También deben considerarse procedimientos para los siguientes servicios que son de uso y/o consulta de los usuarios:

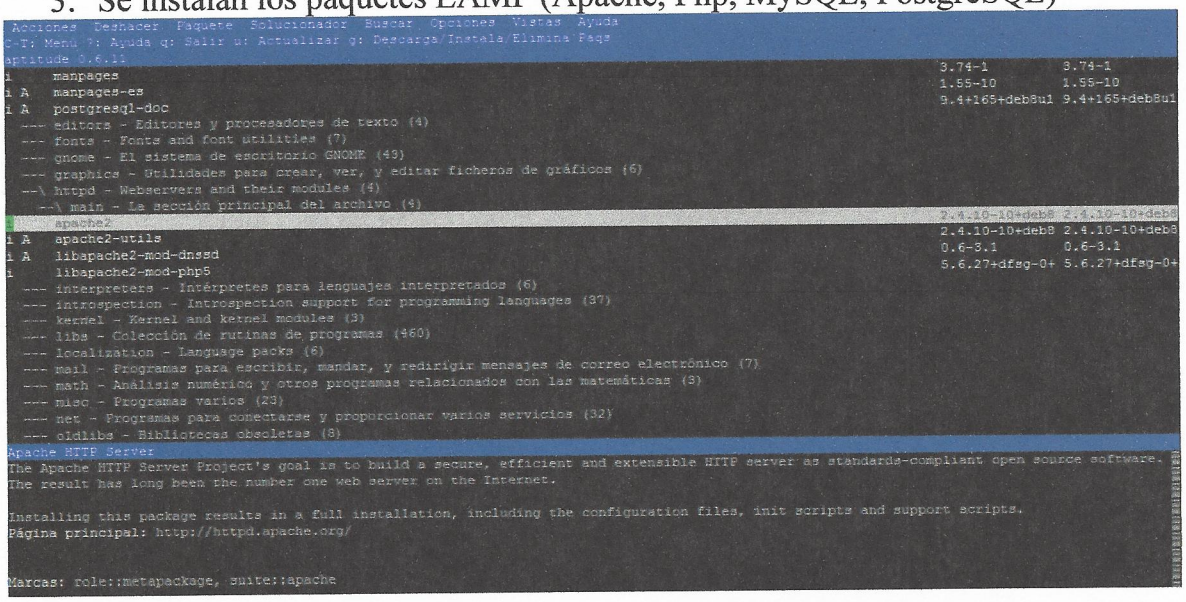
- Recuperación del Servicio Web e Intranet.
- Recuperación del Servidor de Correo.
- Recuperación ante la falla de equipos firewall.
- Recuperación de falla de servidor de aula virtual.

ACTIVIDADES A REALIZAR PARA SUPLIR LA CONTINGENCIA

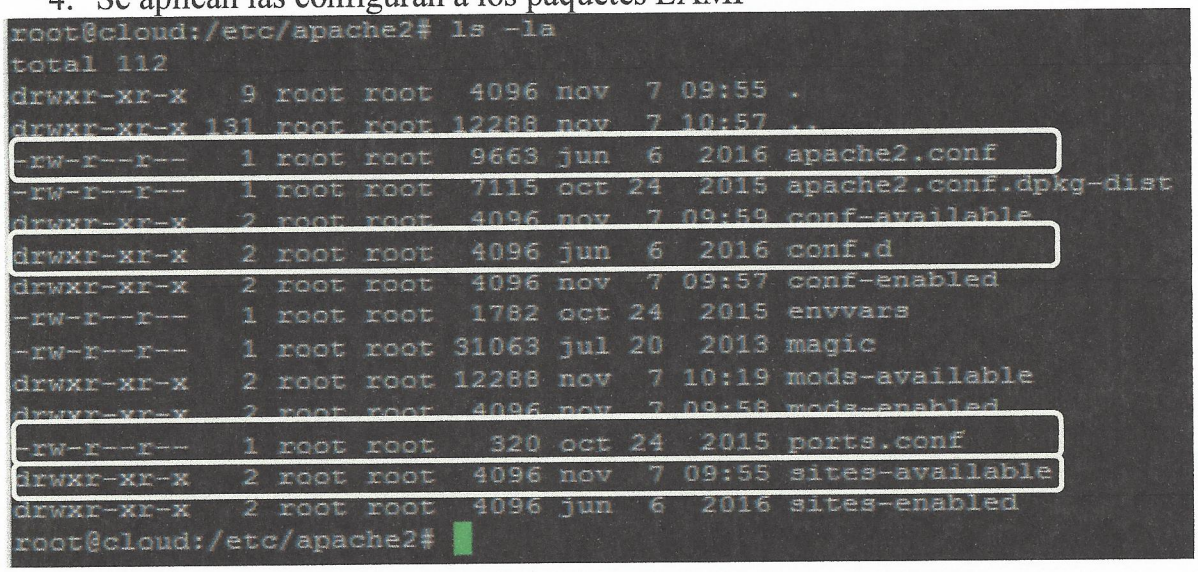
1. Recuperación de las aplicaciones en producción.

Si el problema que presenta el servidor un fallo general de Sistema Operativo

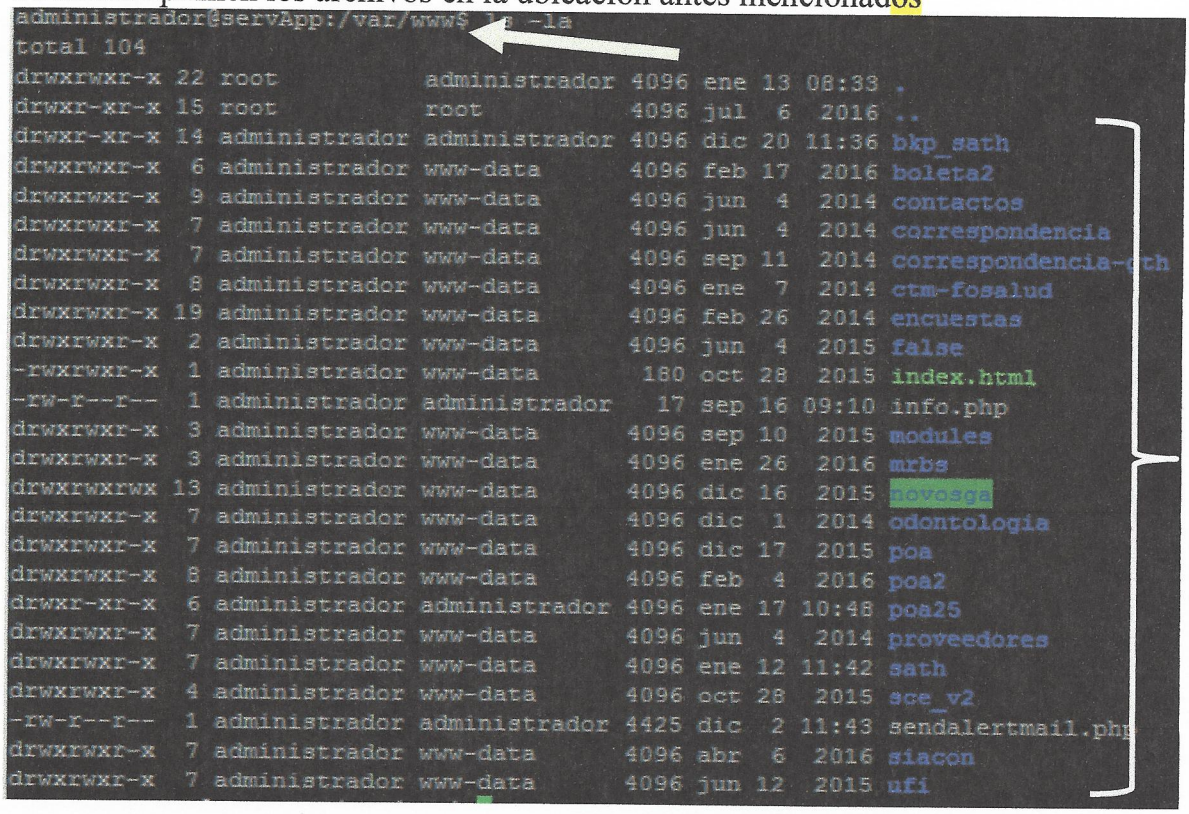
1. Si es falla general de Sistema Operativo, se procede a la reinstalación completa del sistema operativo.
2. Se realizan las configuraciones básicas del Sistema Operativo
3. Se instalan los paquetes LAMP (Apache, Php, MySQL, PostgreSQL)



4. Se aplican las configuran a los paquetes LAMP



5. Del repositorio de respaldos, se copian los archivos comprimidos de las aplicaciones web y se pegan en la ubicación /var/www/ del servidor de aplicaciones
6. Se descomprimen los archivos en la ubicación antes mencionados



7. Del repositorio de respaldos, se copia la última copia de respaldo realizada a la base de datos
8. Se ejecuta el script de base de datos, para realizar la restauración de las bases de datos de las aplicaciones

"*mysql –u root –p < respaldo-completo-bases.sql*"

9. Se comprueba que las aplicaciones queden funcionando correctamente.

Si el problema es un paquete desactualizado o incompatibilidad

1. Se procede a determinar que paquete está provocando un error en el servicio de aplicaciones
2. Si el paquete esta desactualizado y no permite funcionar correctamente los paquetes LAMP, se procede a su actualización
3. Si el paquete no es necesario y por motivos de compatibilidad no permite el correcto funcionamiento de los servicios, se procede a desinstalar el paquete

Si el problema que presenta el servidor es hardware

1. Se prepara un servidor temporal con prestaciones mínimas para su funcionamiento con el paquete LAMP y se configura para su uso
2. Se migran los sistemas y las bases de datos a un servidor temporal, para que los usuarios puedan seguir trabajando sobre los sistemas
3. Se gestiona con el jefe de la Unidad de Tecnología de Información, la reparación del servidor, en caso no se pueda reparar se gestiona la compra de un servidor nuevo o la creación de un servidor virtual.
4. Una vez el servidor se encuentre funcionando (Virtual o Físico), se migran los sistemas y las bases de datos del servidor temporal al nuevo servidor asignado para esta función.

2. Recuperación de datos de los usuarios.

1. A través del servicio de soporte técnico se verifica la falla del equipo reportado, si el daño es lógico o de sistema operativo debe realizarse un respaldo de la información y reinstalar el equipo. Si el daño es físico se debe abrir un caso con la empresa responsable del mantenimiento correctivo para la reparación del equipo.
2. Si el daño físico detectado ha ocurrido en el disco duro y se ha ocurrido pérdida total, deberá utilizarse el sistema Exec Backup Symactec Desktop and Laptop Option.
3. Se debe restaurar la última actualización realizada a dicho equipo y copiarla al equipo reparado.

3. Recuperación del Servicio Web e Intranet.

El presente manual se utilizará para sitio web institucional e Intranet, debido a que los dos sitios web utilizan el mismo gestor de contenidos. En su misma versión actualizada.

Fallo general de Sistema Operativo

1. Si es falla general de Sistema Operativo, se procede a la reinstalación completa del sistema operativo.
2. Se realizan las configuraciones básicas del Sistema Operativo
3. Se instalan los paquetes LAMP (Apache, Php, MySQL, PostgreSQL)
4. Se aplican las configuran a los paquetes LAMP
5. Se realiza instalación de estándar de wordpress, se copian los archivos comprimidos de los respaldos web y se pegan en la ubicación /var/www/ del servidor de sitio Web.

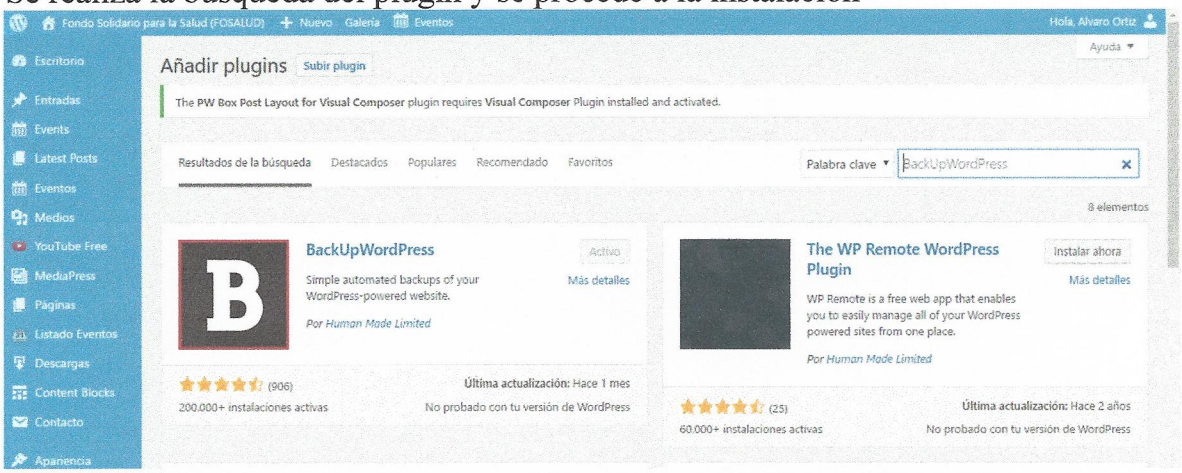
6. Se descomprimen los archivos en la ubicación antes mencionada
7. Del repositorio de respaldos, se copia la última copia de respaldo realizada a la base de datos
8. Se ejecuta el script de base de datos, para realizar la restauración de las bases de datos de las aplicaciones
9. Se comprueba que el sitio web quede funcionando correctamente.

Configuración de Respaldo Diario.

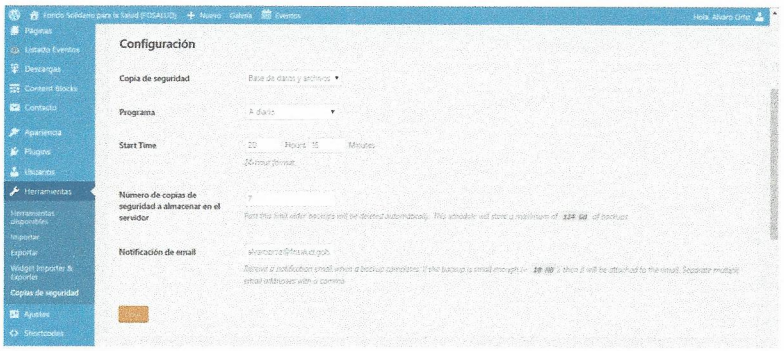
Previamente se ha instalado el plugin Back Up Wordpress el cual se especializa en la creación de un backup WordPress para el sitio de forma sencilla y automatizada.

Adecuación de Plugin para respaldo:

1. Ingresar al dashboard de administración de WordPress.
2. Se realiza la búsqueda del plugin y se procede a la instalación



3. Para programar un respaldo automático, hacemos clic en **BackWPup > Configuración**. Realiza primero los ajustes generales de la creación del backup WordPress. Elegimos el tipo de respaldo, para el caso del sitio web institucional se ha escogido la opción **Base de datos y archivos**. Esta opción nos permite tener una copia completa de la base de datos y una copia de los archivos (imágenes, entradas y otras modificaciones) de nuestro sitio web.
   Se elige Frecuencia con que se realiza el respaldo. Se ejecuta a **diario a las 8:00pm** Debido a la cantidad de información que puede ser actualizada por el área de comunicaciones.



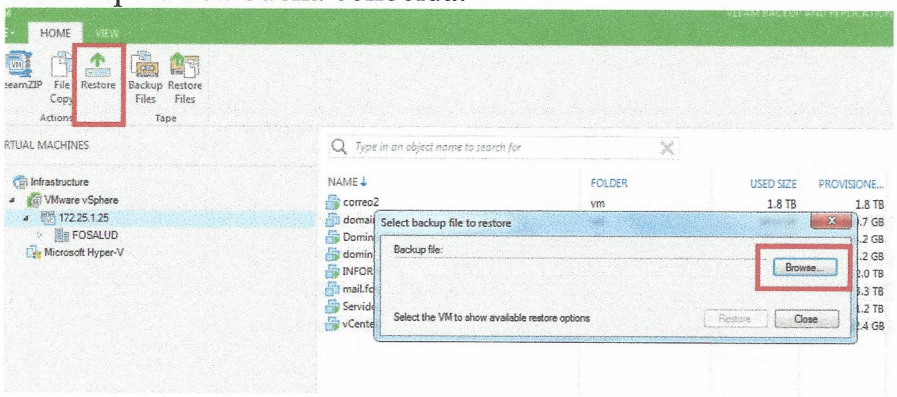
4. Se guarda configuración.

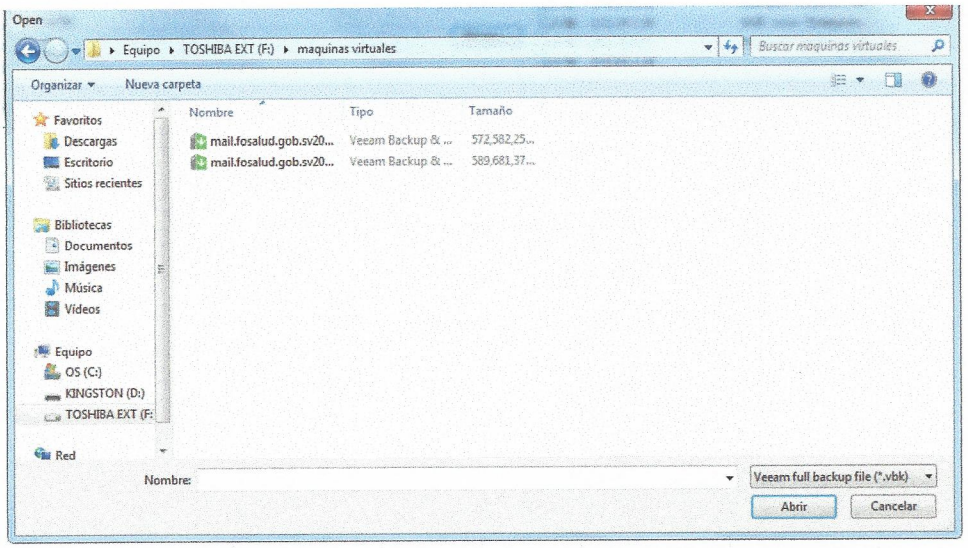
Restauración Respaldo Diario.

1. El primer paso es identificar la base de datos que está utilizando el sitio de Institucional de WordPress.
2. Ejecutar el script de respaldo.
3. Instalación estándar de Wordpress en el directorio /var/www/
4. Localizar los datos de respaldo y sustituirlos por los de la actualización estándar de wordpress.
5. Verificar que coincidan los datos de configuración de base de datos en el archivo **wp-config.php**
6. Se comprueba que el sitio web quede funcionando correctamente.

4. Recuperación del Servidor de Correo.

1. Se verifica a que nivel es la falla del servicio, si el problema es muy grande por daño al sistema se debe proceder con una recuperación del servicio con el último respaldo funcional conocido.
2. Se utilizará la herramienta Veem Backup and Replication en su última versión estable y Free Edition para poder crear respaldos y restaurarlos.
3. Se debe restaurar el respaldo mediante la opción "restore" y seleccionando la última recuperación buena conocida.



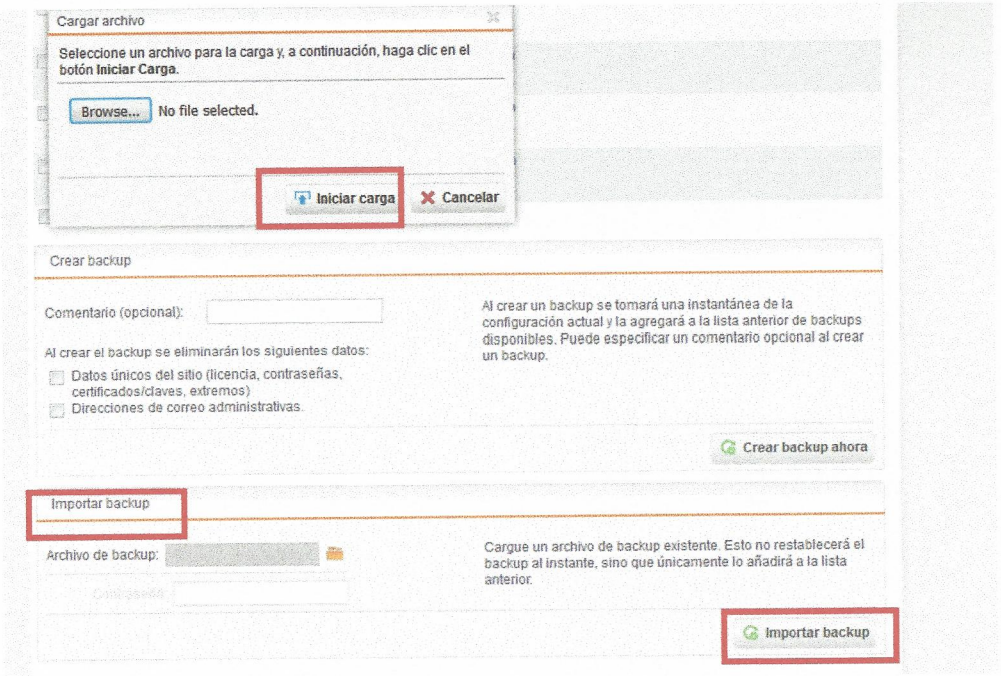


4. Con el respaldo cargado y el nuevo servidor encendido se debe comentar la dirección MAC del archivo /etc/sysconfig/network-scripts/ifcfg-ethX (X es el número de la interface conectada a la red DMZ).
5. Finalmente se debe reiniciar el sistema y el servicio debe estar activo nuevamente.
6. Como paso adicional para reducir la perdida de la información, en la medida de lo posible y siempre que el daño en sistema lo permita, se debe copiar la carpeta zimbra entre los servidores (del servidor en producción al servidor restaurado) ubicada en el directorio /opt/zimbra y reinstalar el servicio con los archivos de instalación de la última versión de zimbra collaboration que se encontraran en la carpeta /opt o con arhivos descargados de la web https://www.zimbra.com/ si existe una nueva versión estable a la existente en la carpeta /opt (para este último paso se deben copiar estos archivos a este directorio y dejarlos ahí para posteriores reinstalaciones que sean necesarias).

   Nota: Se debe mantener respaldos de dicho servidor al menos de la semana anterior y la última semana de los dos meses anteriores. Los respaldos se deberán realizar en caliente ya que la herramienta lo permite.

5. Recuperación ante la falla de equipos firewall

1. Si se detectan problemas con los equipos firewall se debe identificar si la falla se debe a problemas de red o problemas de hardware.
2. Ante problemas de red el equipo debe reiniciarse y monitorear los diferentes sistemas internos (CPU, Memoria, IPS, etc.) para encontrar el problema.
3. Si el problema es de hardware se debe gestionar otro equipo con la empresa que está brindando el soporten o habilitar el equipo de contingencia, con el ultimo respaldo de configuraciones.



Nota: El firewall de la sede debe considerar un sistema redundante (el cual debe ser probado periódicamente) y para los firewalls de los almacenes se debe considerar respuestas de 4 horas ante fallos de hardware verificando la integridad de los backup realizados de las configuraciones.

6. Recuperación del aula virtual

Si el problema que presenta el servidor un fallo general de Sistema Operativo y/o de Hardware del servidor

1. Se procede a la reinstalación completa del sistema operativo.
2. Reinstalar moodle 2.9 o superior cumpliendo los requerimientos: https://docs.moodle.org/all/es/Instalación_de_Moodle#Software
3. Se deben recuperar las copias de seguridad comenzando por el sitio y después con los cursos:
    a. copia_de_seguridad-moodle2-course-1-fosalud-elearning-fecha-hora.mbz
    b. copia_de_seguridad-moodle2-course-6-cbem-fecha-hora.mbz
    c. copia_de_seguridad-moodle2-course-7-investigación-fecha-hora.mbz
    d. copia_de_seguridad-moodle2-course-8-normativas-fecha-hora.mbz
    e. copia_de_seguridad-moodle2-course-9-electro-fecha-hora.mbz

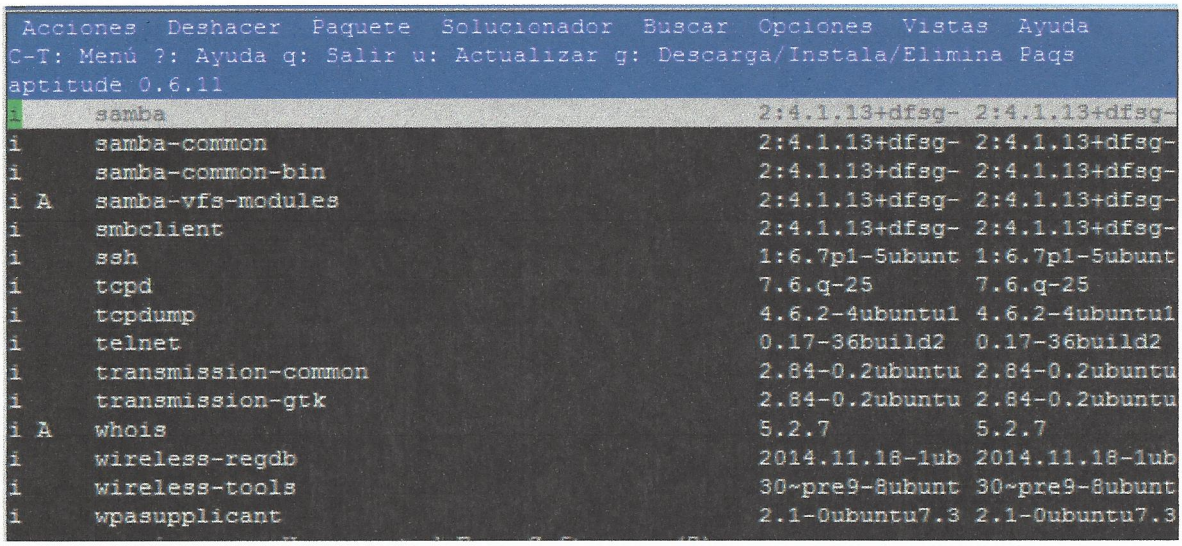
4. Verificar los cursos.

Los problemas de hardware se atenderán con apoyo de la sección de administración de activos y soporte tecnológico.

7. Recuperación de Datos de Directorios Compartidos.

Si el problema que presenta el servidor un fallo general de Sistema Operativo y/o de Hardware del servidor

1. Si es falla general de Sistema Operativo, se procede a la reinstalación completa del sistema operativo.
2. Se realizan las configuraciones básicas del Sistema Operativo
3. Se instalan los paquetes SAMBA



4. Se configuran los grupos Linux y Usuarios Linux
    a. Se agregan los grupos Linux
        1. "*addgroup nombre del grupo*"
    b. Se agregan los usuarios Linux y de asignan a los grupo creados
        1. "*adduser nombre de usuario --group nombre de grupo creado*"
5. Del repositorio de respaldos, se copian los archivos comprimidos de las carpetas usadas como medios compartidos
6. Los archivos se descomprimen los archivos en */home/shared/*esto puede tardar hasta 3 horas dependiendo de la cantidad de información a descomprimir

    "*tar --xzf *.tar.gz*"

7. Con los archivos descomprimidos, se procede a modificar la configuración de SAMBA para compartir las ubicaciones descomprimidas
    a. Configuración Global de SAMBA. Ejemplo:

```
[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
        server string = %h server (Samba, Ubuntu)

#No permitir archivos especiales
veto files = /*.mp3/*.exe/*.pif/*.bat/*.inf/*.zip/

#pwrite pread

vfs objects         = recycle full_audit
full_audit:prefix   = %u|%I|%m|%S
full_audit:success  = mkdir rename unlink rmdir write
full_audit:failure  = none
full_audit:facility = local0
full_audit:priority = INFO

#Recycle
   recycle:repository = /tmp/Trash/%u
   recycle:versions   = TRUE
   recycle:keeptree   = TRUE
   recycle:touch      = FALSE
   recycle:exclude    = *.tmp | *.o | ~$* | *.~?? | *.log
   recycle:excludedir = /tmp  | /cache
   recycle:noversions = *.dat | *.ini
   recycle:minsize    = 512
   recycle:maxsize    = 52428800
#50MB maximo de reciclaje (52428800 bytes)
```

b. Configuración de carpetas compartidas. Ejemplo

```
[control de personal]
path = /home/shared/th/ctlpersonal
comment = Control de Personal
   browseable = yes
   read only = no
   guest ok = no
   comment = Control de Personal
   browseable = yes
   writable = yes
   available = yes
   read only = no
   create mask = 0775
   directory mask = 0775
   valid users = @ctlpersonal
   write list = @ctlpersonal
   force group = ctlpersonal
   force mode = 775
   force directory = 775
```

8. Se comprueba que las sesiones estén activas y que puedan ingresar a las carpetas en las que contiene permisos.

Los problemas de hardware se atenderán con apoyo de la sección de administración de activos y soporte tecnológico.

UBICACIÓN Y ACCESOS DE LOS RESPALDOS Y/O REPOSITORIOS DE DATOS.

No.	Procedimiento de recuperación	Responsable del Repositorio	Ubicación de las fuentes, respaldos y/o repositorios.
1	Recuperación de las aplicaciones en producción.	Ing. Carlos Fuentes	Servidor de respaldo (10.0.0.20)
2	Procedimiento para la recuperación de datos de los usuarios.	Álvaro Ortiz	Servidor DLO (192.168.100.113)
3	Recuperación del Servicio Web e Intranet.	Álvaro Ortiz	Servidor Web de Respaldo (10.0.0.8)
4	Recuperación del Servidor de Correo.	Ing. Nelson Najarro	En equipo del Jefe UTI Respaldos últimas semanas: - BK1- Disco Externo para respaldo. Respaldo último dos meses (última semana de cada mes): - BK2- Disco Externo para Respaldo.
5	Recuperación ante la falla de equipos firewall.	Ing. Nelson Najarro	Archivos de configuración se remitirán a los correos de Ing. Najarro e Ing. Fuentes.
6	Recuperación de falla de servidor de aula virtual.	Ing. Nelson Najarro	En equipo del Jefe UTI BK2- Disco Externo para Respaldo.
7	Recuperación de Datos de Directorios Compartidos.	Ing. Carlos Fuentes	Disco Duro externo 1TB ubicado en puerto USB de servidor de medios compartidos

- Los repositorios estarán en un equipo separado del servidor donde el servicio se está ejecutando, el responsable deberá monitoreará que s estos se realicen de forma íntegra y que solo sean accedidos por él y por el personal alterno responsable de la recuperación del servicio.

PERSONAL TÉCNICO Y ENCARGADO RESPONSABLES.

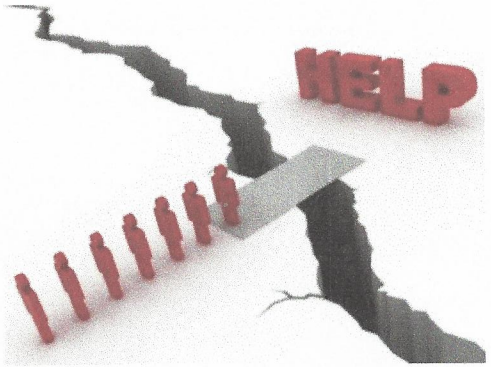
No.	Procedimiento de recuperación	Responsable de Ejecución	Personal alterno para recuperar ejecución
1	Recuperación de las aplicaciones en producción.	Ing. Carlos Fuentes	Ing. William Rivera
2	Procedimiento para la recuperación de datos de los usuarios.	Álvaro Ortiz	Ing. Nelson Najarro
3	Recuperación del Servicio Web e Intranet.	Álvaro Ortiz	Ing. William Rivera
4	Recuperación del Servidor de Correo.	Ing. Nelson Najarro	Ing. Carlos Fuentes
5	Recuperación ante la falla de equipos firewall.	Ing. Nelson Najarro	Ing. Carlos Fuentes
6	Recuperación de falla de servidor de aula virtual.	Ing. Nelson Najarro	Álvaro Ortiz
7	Recuperación de Datos de Directorios Compartidos.	Ing. Carlos Fuentes	Ing. William Rivera

CRONOGRAMA DE PRUEBAS DE LOS PLANES

		Resposable	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Pruebas del Responsable de la Ejecución Servicio	Recuperación de las aplicaciones en producción.	Ing. Fuentes										
	Procedimiento para la recuperación de datos de los usuarios.	Alvaro Ortiz										
	Recuperación del Servicio Web e Intranet.	Alvaro Ortiz										
	Recuperación del Servidor de Correo.	Ing. Najarro										
	Recuperación ante la falla de equipos firewall.	Ing. Najarro										
	Recuperación de falla de servidor de aula virtual.	Ing. Najarro										
	Recuperación de Datos de Directorios Compartidos.	Ing. Fuentes										
Propuesta de Actualizaciones / Mejoras		Ing. Najarro										
Pruebas del Personal alterno para recuperar ejecución	Recuperación de las aplicaciones en producción.	Ing. Rivera										
	Procedimiento para la recuperación de datos de los usuarios.	Ing. Najarro										
	Recuperación del Servicio Web e Intranet.	Ing. Rivera										
	Recuperación del Servidor de Correo.	Ing. Fuentes										
	Recuperación ante la falla de equipos firewall.	Ing. Fuentes										
	Recuperación de falla de servidor de aula virtual.	Alvaro Ortiz										
	Recuperación de Datos de Directorios Compartidos.	Ing. Rivera										
Informe de Cierre de la actividad.		Ing. Najarro										

- El responsable de la actividad realizara un informe que formara parte de la ejecución y seguimiento del plan. Como mínimo en la actividad se verificará la integridad de los respaldos y las rutinas de recuperación del servicio.

Plan de Contingencias 2017



Marzo 2017

Base Legal del Manual.

Decreto 22, Corte de Cuentas de la Republica:

- Art. 40. El área TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permita tener acceso a la misma durante periodos de contingencia, causados por desperfectos de los equipos, pérdidas de información u otras situaciones similares.

¿Por qué debe ser aprobado?:

Decreto 22, Corte de Cuentas de la República:

- Art. 39. La Unidad de TIC, deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad, este plan debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la unidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para restablecimiento de las operaciones tecnológicas, este plan debe Probarse, actualizarse atendiendo la realidad tecnológica de la entidad al menos un vez al año. Deberá ser comunicado a los niveles pertinentes.

Estructura del Manual

1. Introducción
2. Objetivos del Manual
3. Alcances del Manual de Contingencias
4. Riesgos Detectados
5. Actividades a realizar para suplir la contingencia
6. Ubicación de los respaldos y/ repositorios con su responsable
7. Persona técnico responsable de los servicios y realizar las actividades para suplir la contingencia.
8. Cronograma 2017 de pruebas del plan y actualizaciones detectadas por los encargados.