



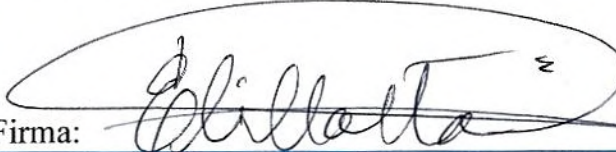
**FONDO SOLIDARIO PARA LA SALUD
FOSALUD.**

**PLAN DE CONTIGENCIAS 2018 PARA
SERVICIOS INFORMATICOS
PROPORCIONADOS POR LA
UNIDAD DE TECNOLOGIAS DE
INFORMACION**

**San Salvador, 7 de marzo de 2018.
Gerencia Administrativa.**

CONTENIDO.

INTRODUCCIÓN.....	4
OBJETIVOS DEL MANUAL.....	4
ALCANCE.....	4
RIESGOS DETECTADOS.....	5
ACTIVIDADES QUE DEBEN CONSIDERARSE EN EL PLAN PARA MINIMIZAR LA CONTINGENCIA.....	8
1. Procedimiento para la recuperación de datos de los usuarios.....	11
2. Procedimiento de Recuperación de Directorios compartidos.....	11
3. Procedimiento de Recuperación de Sitio Web e Intranet.....	13
4. Procedimiento de Recuperación de Aula Virtual.....	14
5. Recuperación de las aplicaciones en producción.....	15
6. Procedimiento de Recuperación de Correo Electrónico.....	16
UBICACIÓN Y ACCESOS DE LOS RESPALDOS Y/O REPOSITORIOS DE DATOS.....	18
PERSONAL TÉCNICO Y ENCARGADO RESPONSABLES.....	19
CRONOGRAMA DE PRUEBAS DE LOS PLANES.....	21

Fecha elaboración:	Responsable de elaboración: Ing. Nelson Eduardo Najarro Alvarez. Jefe de la Unidad de Tecnologías de Información Firma: 
Aprobación por la Dirección Ejecutiva.	Responsable revisión: Ing. Benigno Andrés Mercado Gerente Administrativo Firma: 
Aprobación por la Dirección Ejecutiva.	Responsables 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.

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/técnicos de la unidad de tecnología, con vigencia para el 2018 o hasta que se actualice uno nuevo (2019).

RIESGOS DETECTADOS

Línea Estratégica	Supuesto*	Riesgo Potencial	Causas que originan el riesgo	Probabilidad de Ocurrencia (1-5)	Nivel de Impacto (1-5)	Nivel de Riesgo	Acción recomendada	Actividad para mitigar o eliminar riesgo	Responsable
Integrar y participar activamente en la comisión de tecnologías de la Información de la Hoja de Ruta del SNIS	La institución participan de las acciones conjuntas	La institución no participan de las acciones conjuntas	Acumulación de actividades/responsabilidades para asistir a las reuniones o implementar las nuevas actividades.	1	3	MUY BAJO	Aceptar	Se acepta el riesgo	Nelson Najarro
	Se tiene una respuesta oportuna a los usuarios	Demora en la respuesta técnica a usuarios	fallos de los equipos, perdida de conexión de internet.	3	4	MODERADO	Monitorear	Identificar y registrar incidentes y problemas de TIC reportados por usuarios	Alvaro Ortiz
Implementar mecanismos de participación ciudadana mediante recursos virtuales	La información se encuentra disponible y protegida ante perdidas.	Perdidas de información por defectos en equipos	fallos de los equipos	2	5	MODERADO	Monitorear	Definir y actualizar políticas para el respaldo y recuperación de la información	Alvaro Ortiz
	Los datos son unicos y no estan repetidos en los sistemas.	Generación de datos redundantes o repetitivos.	Errores de digitación en los sistemas, tablas sin relacion de los datos.	3	5	ALTO	Elaborar plan de respuesta	Implementar acciones que permitan garantizar la seguridad lógica a las bases de	Carlos Fuentes

prioritarias de la institución.

					datos institucionales			
Desarrollar soluciones informáticas ante las necesidades prioritarias de la institución.	Sistemas confiables.	Falta de fiabilidad de los sistemas	Liberación de versiones antiguas, pérdida de continuidad entre las versiones liberadas.	2	5	Elaborar e implementar procedimientos de control para gestionar la configuración, cambios y liberación de versiones de software mediante la definición de planes y políticas.	Carlos Fuentes	
						MONITOREAR		
Implementar y socializar la política de seguridad de la información	Personal conoce sus responsabilidades para mitigar los riesgos de la información.	El personal desconoce los riesgos en la seguridad de la información	Personal no leer las normativas vigentes	4	5	Elaborar plan de respuesta	Socializar y sensibilizar sobre la importancia de la aplicación de la política de seguridad	Nelson Najarro
						MUY ALTO		
Implementar y socializar la política de seguridad de la información	Se aplica correctamente las medidas de seguridad de la información por parte de los usuarios.	No se implementa una correcta administración de la seguridad de la información por parte de usuarios	Falta de controles suficientes, falta de definición de políticas,	2	5	Monitorar	Definir controles en la gestión de la información que permitan que la información cumpla con integridad, disponibilidad y confiabilidad	Nelson Najarro
						MODERADO		

Brindar soporte y actualización permanente a la intranet institucional	Los portales se encuentran disponibles para consultar la información.	Fallas en la continuidad de las operaciones	Falta de procedimiento claro para recuperar el servicio.	2	5	MODERADO	Monitorear	Elaborar plan contingencia	Alvaro Ortiz
Desarrollar e implementar el plan de renovación de equipos	Políticas de accesos a sistemas de información y acceso a equipos.	Perdidas en la seguridad física y lógica de los recursos	Falta de canales de comunicación adecuados entre la unidad de tecnología y la Gerencia de Talento Humano. Falta de conocimiento y empoderamiento de las herramientas por parte de los administradores de los sistemas.	2	5	MODERADO	Monitorear	Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos	Nelson Najarro
Desarrollar e implementar el plan de renovación de equipos	Usuarios cuenta con equipos informáticos sin importar los imprevistos.	Siniestralidades en equipos por desastres naturales	Falta de riesgos contemplados en la contratación de los seguros.	3	5	ALTO	Elaborar plan de respuesta	Elaborar diagnóstico de necesidades de seguros	Emmanuel Avelar
Diseñar plan de formación	Las capacitaciones otorgadas apoyan el trabajo de la unidad.	No se realiza un adecuado diagnóstico de necesidades	Falta de una buena investigación de capacitaciones disponibles y desconocimiento del trabajo de las secciones de la unidad.	1	3	MUY BAJO	Aceptar	Se acepta el riesgo	Nelson Najarro
Implementar el plan de formación del personal de TIC	Personal de la unidad participa en las jornadas de capacitación.	No se cuenta con el tiempo para asistir a capacitaciones	No se cuenta con una adecuada planificación de actividades.	1	4	MUY BAJO	Aceptar	Se acepta el riesgo	Nelson Najarro

ACTIVIDADES QUE DEBEN CONSIDERARSE EN EL PLAN PARA MINIMIZAR LA CONTINGENCIA.

Sobre la base de estos riesgos se realiza un análisis sobre las actividades que deben desarrollarse como parte del Plan de contingencias, los riesgos a cuáles no se les liste actividad será porque corresponden a otro ámbito, tales como definición de políticas, normativas, lineamientos, etc.

<i>Línea Estratégica</i>	Supuesto*	Riesgo Potencial	Actividad para mitigar o eliminar riesgo	Responsable	Actividades que se desarrollará como parte del plan de contingencias para mitigar el riesgo.
Integrar y participar activamente en la comisión de tecnologías de la Información de la Hoja de Ruta del SNIS	La institución participan de las acciones conjuntas	La institución no participan de las acciones conjuntas	<u>Se acepta el riesgo</u>	Nelson Najarro	No se considera actividad en este documento, ya que el riesgo no es significativo.
Mantener una actualización permanente y novedosa de la página web institucional	Se tiene una respuesta oportuna a los usuarios	Demora en la respuesta técnica a usuarios	Identificar y registrar incidentes y problemas de TIC reportados por usuarios	Alvaro Ortiz	No se considera actividad en este documento ya que el riesgo es relativo al registro de los problemas de los usuarios en los relacionado al sitio web.
Implementar mecanismos de participación ciudadana mediante recursos virtuales	La información se encuentra disponible y protegida ante pérdidas.	Perdidas de información por defectos en equipos (computadoras y servidores)	Definir y actualizar políticas para el respaldo y recuperación de la información	Alvaro Ortiz	<ul style="list-style-type: none"> - Procedimiento de Recuperación de Sitio Web e Intranet. - Procedimiento para la recuperación de datos de los usuarios. - Procedimiento de Recuperación de Aula Virtual. - Procedimiento de Recuperación de Correo Electrónico. - Recuperación de directorios compartidos.

Desarrollar soluciones informáticas ante las necesidades prioritarias de la institución.	Los datos son unicos y no estan repetidos en los sistemas.	Generación de datos redundantes o repetitivos.	Implementar acciones que permitan garantizar la seguridad lógica a las bases de datos institucionales	Carlos Fuentes	Procedimiento de Recuperación de Servidor de Aplicaciones
Desarrollar soluciones informáticas ante las necesidades prioritarias de la institución.	Sistemas confiables.	Falta de fiabilidad de los sistemas	Elaborar e implementar procedimientos de control para gestionar la configuración, cambios y liberación de versiones de software mediante la definición de planes y políticas.	Carlos Fuentes	No se considera actividad en este documento ya que el riesgo es relativo a la implementación de políticas y normativas.
Implementar y socializar la política de seguridad de la información	Personal conoce sus responsabilidades para mitigar los riesgos de la información.	El personal desconoce los riesgos en la seguridad de la información	Socializar y sensibilizar sobre la importancia de la aplicación de la política de seguridad	Nelson Najarro	No se considera actividad en este documento ya que el riesgo es relativo a dar a conocer al personal políticas y normativas.
Implementar y socializar la política de seguridad de la información	Se aplica correctamente las medidas de seguridad de la información por parte de los usuarios.	No se implementa una correcta administración de la seguridad de la información por parte de usuarios	Definir controles en la gestión de la información que permitan que la información cumpla con integridad, disponibilidad y confiabilidad	Nelson Najarro	No se considera actividad en este documento, ya que el riesgo es relativo a verificar que se cumplan las políticas emitidas.
Brindar soporte y actualización permanente a la intranet institucional	Los portales se encuentran disponibles para consultar la información.	Fallas en la continuidad de las operaciones	Elaborar plan contingencia	Alvaro Ortiz	Procedimiento de Recuperación de Sitio Web e Intranet

Desarrollar e implementar el plan de renovación de equipos	Políticas de accesos a sistemas de información y acceso a equipos.	Perdidas en la seguridad física y lógica de los recursos	Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos	Nelson Najarro	No se considera actividad en este documento, ya que el riesgo es relativo a establecer políticas y normativas de autorización de accesos.
Desarrollar e implementar el plan de renovación de equipos	Usuarios cuenta con equipos informáticos sin importar los imprevistos.	Siniestralidades en equipos por desastres naturales	Elaborar diagnóstico de necesidades de seguros	Emmanuel Avelar	No se considera actividad en este documento , ya que el riesgo es sobre el diagnósticos de necesidades de seguros.
Diseñar plan de formación	Las capacitaciones otorgadas apoyar el trabajo de la unidad.	No se realiza un adecuado diagnóstico de necesidades	<u>Se acepta el riesgo</u>	Nelson Najarro	No se considera actividad en este documento, ya que el riesgo no es significativo.
Implementar el plan de formación del personal de TIC	Personal de la unidad participa en las jornadas de capacitación.	No se cuenta con el tiempo para asistir a capacitaciones	<u>Se acepta el riesgo</u>	Nelson Najarro	No se considera actividad en este documento, ya que el riesgo no es significativo.

Sobre el análisis anterior las actividades a desarrollar son las siguientes:

1. Procedimiento para la recuperación de datos de los usuarios.
2. Procedimiento de Directorios compartidos.
3. Procedimiento de Recuperación de Sitio Web e Intranet
4. Procedimiento de Recuperación de Aula Virtual
5. Procedimiento de Recuperación de Servidor de Aplicaciones
6. Procedimiento de Recuperación de Correo Electrónico

1. Procedimiento para la recuperación de datos de los usuarios.

Restauración de datos de usuarios.

Esta prueba parte del hecho que luego del diagnostico realizado por la unidad de tecnologia, el equipo presenta un problema de hardware irreparable. Por lo que se procede a recuperar los datos del sistema de respaldo.

Nombre del Usuario a quien se le restauraran los datos:

- Ingresar al servidor 192.168.100.113
- Abrir la plataforma DLO
- Seleccionar el usuario a restaurar.
- Seleccionar los datos del Usuario
- Seleccionar la ubicación
- Iniciar el proceso de restauración
- Iniciar el Procedimiento Hora: _____
- Verificar que el procedimiento concluyo con éxito. Hora: _____

Observaciones:

Nombre, Sello y Firma

2. Procedimiento de Recuperación de Directorios compartidos.

Lista de Chequeo Plan de Contingencia A

• Instalación de Sistema Operativo

Indicar que distribución Linux se Instaló:

- Debian
- Ubuntu

Versión: _____
Tiempo de instalación: _____

• **Instalación de LAMP [Apache Es utilizado para servicio ownCloud**

Tiempo de instalación: _____

• **Instalación de Servicio SAMBA**

Instalación de Servicios SAMBA: _____

• **Copia y Restauración de Archivos SAMBA**

Copia de carpeta home/* : _____

Descompresión de archivos: _____

• **Restauración de Configuraciones**

/etc/samba/smb.conf

/var/lib/samba/private/* [Base de datos de contraseña SAMBA]

/etc/apache2/

/etc/hosts

Restauración de archivos de respaldos: _____

• **Restauración de Archivos de Autenticación.**

/etc/shadow

/etc/users

/etc/sh

Restauración de archivos de autenticación SAMBA: _____

• **Restauracion y Configuracion de Servicios Web y OwnCloud**

Owncloud

Apache

Php

MySql

Restauración de configuración y Servicio ownCloud:

• **Pruebas de funcionalidad**

Pruebas exitosas

• **Observaciones:**

Nombre, Sello y Firma

3. Procedimiento de Recuperación de Sitio Web e Intranet

Lista de Chequeo Plan de Contingencia Servidor de Servicios Web

• **Instalación de Sistema Operativo, servicios y aplicativos**

Indicar que distribución Linux se Instaló:

Debian

Ubuntu

Versión _____

• **Instalación de LAMP**

Se Instaló Correctamente

Tiempo de instalación: _____

• **Copia de respaldos desde el servidor de respaldos**

Se Copió Correctamente

• **Restauración de respaldos y configuraciones de servicios en Servidor de Contingencias**

Restauración de respaldos

Configuración de Apache

Configuración Php5

Configuración MySQL

• **Configuración de Bases de datos**

Definir contraseña de usuario Bases de Datos MySQL

• **Desempaquetado de archivos web e Instalación de gestor de contenidos web**

Se realizó el desempaquetado de archivos

• **Definir usuario y contraseña en archivo wp-options**

Se agregó usuario y contraseña de Base datos

• **Observaciones:**

Nombre, Sello y Firma

4. Procedimiento de Recuperación de Aula Virtual

Lista de Chequeo Plan de Contingencia Aula Virtual

Nota: Ubicación de respaldo

Ip servidor contingencia: 10.0.0.8

Directorio archivos: /var/respaldo/aulavirtual /archivos

Directorio Base de datos: /var/respaldo/webfosalud/bases-mysql

• Instalación de Sistema Operativo, servicios y aplicativos

Indicar que distribución Linux se Instaló:

Debian

Ubuntu

Versión: _7.10 Wheezy_

• Instalación de LAMP

Se Instaló Correctamente

Tiempo: _____

• Restauración de respaldo de Base de datos

Configuración MySQL

Tiempo: _____

• Descomprimir archivo de respaldo

Se Copió Correctamente a /var/www/

Descomprimir respaldo.

Tiempo: _____

• Corroborar usuario y contraseña en archivo config.php.

Usuario y contraseña de Base datos correctos

Url del sitio

Url cache del sitio

• Observaciones:

Nombre, Sello y Firma _____

5. Recuperación de las aplicaciones en producción.

Lista de Chequeo Plan de Contingencia Servidor de Aplicaciones

• Instalación de Sistema Operativo, servicios y aplicativos

Indicar que distribución Linux se Instaló:

- Debian
- Ubuntu

Versión: _____

Tiempo de instalación: _____

• Instalación de LAMP

- Tiempo de instalación: _____

• Copia de respaldos

- Desde el servidor de respaldos: _____

• Restauración de respaldos y configuraciones de servicios en Servidor de Contingencias

Restauración de respaldos: _____

- Restauración de configuración de Apache
- Restauración de configuración Php5
- Restauración de configuración MySQL
- Restauración de configuración PostgreSQL

• Configuración de Bases de datos

- Configuración de usuarios y bases de datos Postgres: _____

Restauración de bases de datos

- Bases de Datos Postgres SQL: _____
- Bases de Datos MySQL: _____

• Desempaquetado de archivos e Instalación de aplicaciones web

- Se realizó el desempaquetado de archivos: _____
- Aplicación de grupo www-data y cambio de permisos a 775 en /var/www/* : _____

• Pruebas de funcionalidad

- Pruebas exitosas

• Observaciones:

Nombre, Sello y Firma

6. Procedimiento de Recuperación de Correo Electrónico

Lista de Chequeo Plan de Contingencia de VM - Zimbra

- NOTA: Para realizar respaldos de Máquinas Virtuales (VM) se debe usar Veembackup
- Iniciar Veeam Backup
- Dar Clic en el botón “Restore”
- En la ventana emergente, buscar y seleccionar el archivo de respaldo de la máquina virtual a restaurar
 - Archivo con extensión vbk
 - Muestra detalles de VM: Tamaño (GB), Edad del respaldo, VM contenida
- Con la imagen cargada dar clic en botón “Restore”
 - Seleccionar restaurar VM completa
- Después de la acción anterior, muestra una nueva ventana emergente con las VMs a ser restauradas, dar clic sobre la VM a restaurar y dar clic en el botón “Next >”
 - El detalle de datos mostrados son iguales al paso anterior. Peso, Nombre, Edad de respaldo
- Selección de destino de restauración de VM
 - Seleccionar: “Restaurar en un nuevo destino o con configuraciones diferentes”
 - Verificar que la opción “Restaurar banderas de VM” este seleccionado
 - Clic en botón “Next >”
- Cambiar opciones de Host
 - Cambiar el nombre de la VM
- Opciones de “Resource pool”
 - Verificar
 - Dar clic en el botón “Next >”
- Opciones de Datastore (DS): Cambiar ubicación de DS a la ubicación con espacio para la VM:
 - Archivos de Configuración “Configuration Files”
 - Disco Duro 1 (Hard Disk 1)
 - Disco Duro 2 (Hard Disk 2)
 - Clic en botón “Next >”
- Opciones de Folder
 - Verificar información y dar clic en botón “Next >”
- Opciones de Network
 - Verificar que cuenta con interfaz de red DMZ a ser restaurada
 - Verificar que la interfaz se encuentre desconectada
 - Clic en botón “Next >”

• **Opciones de “Reason”**

- Ingresar la razón por la que se realizara la restauración de la VM seleccionada [Punto de control de auditoria de VMWare]
- Clic en el botón “Next >”

• **Resumen de restauración “Summary”**

- Verificar la información de acciones a realizar por parte de Veeam Backup
- Si todo está acorde a lo seleccionado dar clic en el botón “Next >”

• **Esperar que la restauración finalice para realizar pruebas de la VM restaurada**

• **Iniciar software de administración VMWare**

- La VM restaurada aparece con el nombre ingresado en los pasos anteriores?

• **Configuración de VM restaurada**

- En las propiedades de la Vm verificar la sección de network
- Cambiar la ubicación de red de DMZ a VMNetwork [Lan interna]
- Marcar como conectada la interfaz de red

• **Iniciar la VM restaurada**

- Se inició correctamente la VM restaurada

• **Iniciar la administración de Zimbra en la VM restaurada**

• **Verificar que los servicios de Zimbra se encuentran funcionando. Utilizar comando `zmcontrol status`**

- Todos los servicios están funcionando correctamente

• **Tiempo de restauración total:**

• **Observaciones:**

Nombre, Sello y Firma

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 REPOSITARIOS DE DATOS.

No.	Responsable de los Repositorios de respaldos.	Ubicación de las fuentes, respaldos y/o repositorios.
1	Sr. Alvaro Ortiz	<p>Procedimiento para la recuperación de datos de los usuarios.</p> <p>Directorio: 192.168.100.113- D:\FOSALUD_STORAGE</p>
2	Ing. Carlos Fuentes	<p>Procedimiento de Directorios compartidos.</p> <p>Gestión y vida de respaldos: Respaldos del servidor de producción (10.0.0.12) son realizadas diariamente en horarios 12:45m y 6:00pm</p>
3	Sr. Alvaro Ortiz	<p>Procedimiento de Recuperación de Sitio Web e Intranet</p> <p>Directorio: 10.0.0.8/var/respaldo/webfosalud -archivos -Base datos</p>
4	Sr. Alvaro Ortiz	<p>Procedimiento de Recuperación de Aula Virtual</p> <p>Directorio: 10.0.0.8/var/respaldo/AulaVirtual -archivos -Base datos</p>
5	Ing. Carlos Fuentes	<p>Procedimiento de Recuperación de Servidor de Aplicaciones y directorios compartidos.</p> <p>Sistemas Informáticos [Codigos Fuentes]: Fuentes en respaldo: Servidor IP 10.0.0.20 ubicación: /var/respaldo/servApp/archivos/*</p> <p>Fuentes en desarrollo: Sincronizado via Netbeans con Servidor IP 10.0.0.13 en ubicación: /var/www/*</p> <p>Sistemas Informáticos [Bases de Datos]: Base de Datos en respaldo: Servidor IP 10.0.0.20 ubicación: /var/respaldo/servApp/bases-mysql/*</p>

4	Ing. Nelson Najarro.	Procedimiento de Recuperación de Correo Electrónico
		La ultima copia semanal completa se almacena dentro del disco G: (con capacidad de 2TB) Copias de meses anteriores se almacén en el disco F: (con capacidad de 3TB). Estos en el equipo del Jefe UTI.

- Los repositorios están en un equipo separado del servidor donde el servicio se está ejecutando, el responsable deberá monitorear 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
1	Procedimiento para la recuperación de datos de los usuarios.	Sr. Alvaro Ortiz
2	Procedimiento de Directorios compartidos.	Ing. Carlos Fuentes
3	Procedimiento de Recuperación de Sitio Web e Intranet	Sr. Alvaro Ortiz
4	Procedimiento de Recuperación de Aula Virtual	Sr. Alvaro Ortiz
5	Procedimiento de Recuperación de Servidor de Aplicaciones	Ing. Carlos Fuentes
6	Procedimiento de Recuperación de Correo Electrónico	Ing. Nelson Najarro.
No.	Procedimiento de recuperación	Responsable Secundario de Ejecución (por incapacidad u otro problema en donde el responsable no pueda dar respuesta)
1	Procedimiento para la recuperación de datos de los usuarios.	Ing. Nelson Najarro
2	Procedimiento de Directorios compartidos.	Ing. William Rivera
3	Procedimiento de Recuperación de Sitio Web e Intranet	Ing. William Rivera
4	Procedimiento de Recuperación de Aula Virtual	Ing. William Rivera

5	Procedimiento de Recuperación de Servidor de Aplicaciones	Ing. William Rivera
6	Procedimiento de Recuperación de Correo Electrónico	Ing. Carlos Fuentes

CRONOGRAMA DE PRUEBAS DE LOS PLANES

	Responsible	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Elaboración y gestión de aprobación del PCA de la unidad	Ing. Najarro												
Elaboración y gestión de aprobación del Plan de Contingencias.	Ing. Najarro												
Pruebas del Responsable de la Ejecución Servicio	1. Procedimiento para la recuperación de datos de los usuarios.	Alvaro Ortiz											
	2. Procedimiento de Directorios compartidos.	Ing. Fuentes											
	3. Procedimiento de Recuperación de Sitio Web e Intranet	Alvaro Ortiz											
	4. Procedimiento de Recuperación de Aula Virtual	Alvaro Ortiz											
	5. Procedimiento de Recuperación de Servidor de Aplicaciones	Ing. Fuentes											
	6. Procedimiento de Recuperación de Correo Electrónico	Ing. Najarro											
Informe de Mejoras (si aplican).	Ing. Najarro												
Pruebas del Personal alterno para recuperar ejecución	1. Procedimiento para la recuperación de datos de los usuarios.	Ing. Najarro											
	2. Procedimiento de Directorios compartidos.	Ing. Rivera											
	3. Procedimiento de Recuperación de Sitio Web e Intranet	Ing. Rivera											
	4. Procedimiento de Recuperación de Aula Virtual	Ing. Rivera											
	5. Procedimiento de Recuperación de Servidor de Aplicaciones	Ing. Rivera											
	6. Procedimiento de Recuperación de Correo Electrónico	Ing. Fuentes											
Informe de Cierre	Ing. Najarro												

- 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, las rutinas de recuperación del servicio y tiempos de recuperación.