



RESOLUCIÓN GERENCIAL N°061-2014-GRSM-PEAM-01.00

Moyobamba, 16 MAYO 2014

VISTO:

El Informe N°056-2014-GRSM-PEAM.01.06, del Especialista en Sistemas e Informática - PEAM.

CONSIDERANDO:

Que, mediante Informe N°056-2014-GRSM-PEAM.01.06, el Especialista en Sistemas e Informática hace de conocimiento a esta Gerencia General que, se encuentra considerado como actividad la elaboración de la Directiva: **"Políticas y Procedimientos para el respaldo de la información en el Proyecto Especial Alto Mayo"**; asimismo, con Memorando de Control Interno N°10-2013-GRSM-PEAM, recomienda contar con la mencionada directiva. Dada la importancia de contar con la referida directiva, que permita adecuar los procesos internos del área de informática a las normas técnicas nacionales e internacionales, referentes a la seguridad de la información; por lo que solicita la aprobación vía documento resolutivo de la mencionada Directiva;

Que, estando al proyecto de Directiva sobre: **"Políticas y Procedimientos para el respaldo de la Información en el Proyecto Especial Alto Mayo"** presentada por el Especialista en Sistemas e Informática, el cual tiene por objeto proporcionar un marco operativo y normativo que regule el proceso de respaldo de la información institucional, mantener la integridad y disponibilidad de la información y los medios de procesamiento de la misma, así como garantizar la continuidad de los sistemas de información ante cualquier incidente que afecte la operatividad de la infraestructura de tecnologías de información; resulta procedente la aprobación de la referida Directiva, el cual consta de 37 fojas, con un contenido de 09 puntos y 03 anexos;

Por las consideraciones precedentes y estando a las facultades conferidas por Resolución Ejecutiva Regional N°001-2013-GRSM/PGR, de fecha 02.01.2013, y a lo señalado por el inciso h) del Artículo 15° y demás pertinentes del Manual de Organización y Funciones del Proyecto Especial Alto Mayo, con las visaciones de la Oficina de Presupuesto, Planificación, Estudios y Ordenamiento Territorial y Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo Primero.-APROBAR la Directiva N°008-2014-GRSM-PEAM, **"Políticas y Procedimientos para el respaldo de la Información en el Proyecto Especial Alto Mayo"**; la misma que consta de 37 fojas, con un contenido de 09 puntos y 03 anexos. Se anexa a la presente Resolución y forma parte de esta.



GOBIERNO REGIONAL SAN MARTIN
PROYECTO ESPECIAL ALTO MAYO



RESOLUCIÓN GERENCIAL N° 0161-2014-GRSM-PEAM-01.00

Artículo Segundo.-El Especialista en Sistemas e Informática del PEAM es el encargado de la supervisión y control de la aplicación de la Directiva, aprobada en el Artículo Primero.

Regístrese, comuníquese y archívese.



Ing. Oswaldo Jiménez Salas
Gerente General

PROYECTO ESPECIAL ALTO MAYO

Informática

DIRECTIVA N° 008 - 2014-GRSM-PEAM-01.00



Políticas y Procedimientos para el Respaldo de Información

Versión 1.0

Año 2014



①.

PROYECTO ESPECIAL ALTO MAYO

Informática

DIRECTIVA N° 008 - 2014-GRSM-PEAM-01.00



Políticas y Procedimientos para el Respaldo de Información

Versión 1.0

Año 2014



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 3 de 37

Tabla de Contenido

Introducción	4
1. Propósito	5
2. Alcance	5
3. Objetivos	5
4. Definiciones	6
5. Tipos de Backup.....	7
6. Información a respaldar.....	8
7. Políticas y Normas para el respaldo de Información	11
7.1 Normas del Tiempo Disponible para efectuar las copias de seguridad de la Información	11
7.2 Resguardo físico de los Medios de Almacenamiento Backup y Organización del Ambiente	11
7.3 Control del Registro de los Respaldos de Información realizados	13
7.4 Restauración y comprobación de la Integridad de la Información Respaldada.....	14
7.5 Respaldo de la información de los usuarios finales.....	14
7.6 Normas que regulan las Responsabilidades del Personal encargado	15
CONTROL INTERNO	16
8. Procedimientos y Programación de Backup	16
8.1 Proceso general de Backup	16
8.2 Descripción de los Procedimientos de Backup.....	17
9. Documentos a Utilizar	29
ANEXO 01: FORMATOS DE BITÁCORAS DE CONTROL.....	31
ANEXO 02: ETIQUETA GENERAL DE LOS MEDIOS DE RESPALDO	35
ANEXO 03: DESCRIPCIÓN DE CÓDIGOS	36



10.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0
		Página 4 de 37

Introducción

En la actualidad, las empresas generan grandes cantidades de información a un ritmo creciente. Gracias a la tecnología, ésta información se puede compartir, copiar, enviar desde cualquier lugar, y ser recibida al instante en otro. Por lo mismo, la información se ha convertido en el activo más importante para una organización o empresa, pues representa aspectos específicos de ésta, en un momento o periodo determinado. La manipulación constante de los datos, incrementan su valor, haciéndose necesario mantenerla segura, íntegra y disponible.

Bajo este escenario, el establecimiento de mecanismos que permitan resguardar la información contenida en un computador, se hacen indiscutibles; por lo que, la formulación e implantación de normas y políticas de Backup o copias de seguridad coadyuvan a preservar la integridad de la información, minimizando riesgos que afecten su disponibilidad, ante la pérdida parcial o total de ésta; garantizando la recuperación a estados confiables con el mínimo porcentaje de pérdidas de datos, lo más cercano al momento en el cual, surgió la contingencia, que aseguren la continuidad de las actividades y no afecte el trabajo realizado por los usuarios.



1.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 5 de 37

1. Propósito

El propósito de este documento es definir los lineamientos generales aplicables a respaldos y copias de seguridad de la información; que permitan reducir riesgos y contar con los medios necesarios para afrontar una emergencia de forma rápida y acertada.

2. Alcance

El presente documento aplica a la siguiente información:

- 2.1 Base de datos de los sistemas de información en producción
- 2.2 Imágenes de servidores virtuales (HyperV y VmWare)
- 2.3 Directorio activo
- 2.4 Archivos de configuración de los servidores en producción
- 2.5 Buzones de correo electrónico
- 2.6 Servidor de archivos
- 2.7 Repositorio de Documentos.
- 2.8 Código fuente, ejecutable e instaladores de los sistemas de información
- 2.9 Medios de instalación de software licenciado
- 2.10 Grabaciones de las cámaras de video vigilancia.

3. Objetivos

- 3.1 Proporcionar un marco operativo y normativo que regule el proceso de respaldo de información Institucional.
- 3.2 Mantener la integridad y disponibilidad de la información y los medios de procesamiento de la misma.
- 3.3 Garantizar la continuidad de los sistemas de información ante cualquier incidente que afecte la operatividad de la infraestructura de tecnologías de información.



0.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 6 de 37

4. Definiciones

BACK-UP: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos extraíbles, unidades de cinta), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Copia de respaldo: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables problemas, si se realiza de forma habitual y periódica.

Copias de seguridad: copias de la información en un medio magnético que se almacena en un lugar seguro.

Sistema de información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Base de datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Recuperación: Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Restauración: Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.

Respaldo de la Información: Se puede definir un respaldo de información como una copia exacta de la información en un espacio diferente o medio de almacenamiento masivo que cumpla con las siguientes características: seguro, confiable, efectivo y de fácil manipulación y acceso. Con el objetivo de minimizar los daños causados por eventos inesperados que puedan dañar los datos y afectar el funcionamiento de los sistemas de la Institución.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 7 de 37

CD's: Disco óptico utilizado para almacenar datos en formato digital, sus siglas CD, corresponden a Compact Disc (Disco compacto). Son consistentes en cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos). Pueden almacenar hasta 80 minutos de audio o 700 MB de datos.

DVD's: Disco óptico de almacenamiento de datos. Sus siglas corresponden a Digital Versatile Disc (Disco Versátil Digital). Pueden almacenar hasta 4.7 GB. De información.

Blue Ray: Conocido también como BD (Blue Ray Disc), es un formato de disco óptico de nueva generación. Empleado para vídeo de alta definición y con una capacidad de almacenamiento de datos de alta densidad mayor que la del DVD. Guardaba 25 GB por capa, pero se ha desarrollado uno nuevo que almacena desde 25 a 33,4 GB por capa.

Cintas LTO (Linear Tape Open): tecnología de cinta magnética de almacenamiento de datos, la versión original alcanzaba los 100 GB de datos en un cartucho. La versión 6, publicada en 2012, puede almacenar hasta 2,5 TB en un cartucho del mismo tamaño.

El área de Informática del Proyecto Especial Alto Mayo realizará backup (respaldos) y copias de seguridad de los distintos tipos de información que están definidos en la **sección 2**. Del presente documento, estos serán efectuados en cintas LTO y discos CD, DVD y BlueRay.

5. Tipos de Backup

Existen tres tipos básicos de realizar un backup:

Full Backup o total: Este tipo de backup permite respaldar toda la información seleccionada en un momento determinado. Es decir, si los datos a respaldar nunca cambian, cada respaldo completo será una copia fiel del anterior. Es el tipo de backup que consume más recursos desde el punto de vista de tiempo y almacenamiento, y aunque es el más costoso, también es el más confiable porque no depende sino de sí mismo. Sin embargo a la hora de realizar una recuperación, es mucho más simple porque no debe recurrir a otros backups como referencia para restaurar la información.

①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 8 de 37

Backup Incremental: Este tipo de backup necesita un punto de referencia, el cual se da a través de un backup total, para que a partir de allí se pueda establecer qué información ha cambiado y en qué proporción, y a esa información realizarse un backup, a partir del archivo que cambió. Esta estrategia de backup es más rápida a la hora de respaldar, pero es la más lenta en recuperación, porque el sistema de backup debe armar toda la trayectoria del cambio y eso implica buscar y reunir los medios necesarios, por lo que el proceso en general requiere de tiempo.

Backup Diferencial: Es un tipo de backup que al igual que el anterior, requiere un backup total como punto de partida y a partir de allí determinar qué información ha cambiado, y a esa información en su totalidad realizarse un backups. A diferencia del incremental, el respaldo se hace de todo el archivo que ha cambiado y no solo de la parte modificada dentro del mismo. Es un proceso de backup mucho más rápido que el full backup, más lento que el incremental, pero a nivel de restauración es más rápido que el incremental y más lento que el backup total, porque depende de menos medios para construir la cadena de recuperación.

En el caso particular del Proyecto Especial Alto Mayo, se realizarán Backups del Tipo **Full Backup**; si el software y los equipos de generación de copias de seguridad lo permitan se podrán realizar los otros tipos de backup.

6. Información a respaldar

a. Base de datos de los sistemas de información en producción

Los backups de las bases de datos en producción se realizarán de forma diaria en el servidor de almacenamiento, y una copia semanal, de todos los backups diarios los días lunes, en un medio de almacenamiento externo, Cd, DVD o Cintas, el cual será almacenado en un ambiente fuera del área del servidor.

b. Imágenes de servidores virtuales (HyperV y VmWare)

Las copias de seguridad de las imágenes de servidores virtuales (HyperV y VmWare) se llevarán a cabo de forma mensual (final de cada mes) o cada vez que ocurra algún cambio, en primera instancia en el servidor de almacenamiento, para luego ser copiada en un medio de almacenamiento externo, Blue Ray o Cinta, y ser guardado posteriormente en un ambiente fuera del área del servidor.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0
		Página 9 de 37

c. Directorio activo

Los backups del directorio activo se realizarán de dos formas: Semanal, los días viernes, aplicando un backup de tipo diferencial, éstas se llevarán a cabo en el servidor de almacenamiento. Mensual, se hará un backup completo empleando las copias semanales en el servidor de almacenamiento; la misma que también será guardada en un medio externo (DVD, BlueRay o Cinta) que será trasladado a un ambiente fuera del área de servidores.

d. Archivos de configuración de los servidores en producción

Es necesario respaldar todo tipo de configuraciones, que por lo general se pierden cuando se realizan reinstalaciones del sistema operativo o del software.

Los backup deben incluir archivos de configuración de:

Windows: La carpeta "archivos de programa" y la carpeta que almacena los servicios.

Linux: La carpeta "etc" y la carpeta que almacena los servicios.

Estos backup se deben realizar de forma mensual o ante cualquier cambio o modificación, una copia en el servidor de almacenamiento y otra en un medio externo como DVD's, Blue Ray o Cintas LTO.

e. Buzones de correo electrónico

Se ejecutarán de forma diaria en el servidor de almacenamiento, y se realizará una copia semanal en un medio externo (CD, DVD o Cintas LTO) que será almacenado en un ambiente fuera del área del servidor.

NOTA: Los backups se realizan por cada buzón de correo electrónico.

f. Respaldo del servidor de Archivos

Se tiene previsto el respaldo de la siguiente información:

- Carpetas personales en red y unidades compartidas.
- Scripts de configuración

Los cuáles serán ejecutados de forma semanal en el servidor de almacenamiento, y otra copia de lo resguardado en un medio externo (CD, DVD o Cintas LTO).



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 10 de 37

g. Repositorio de Documentos

Los backups del repositorio de documentos digitalizados se ejecutarán de forma diaria, en el servidor de almacenamiento. Las copias de seguridad, de todos los backups hechos durante la semana, en medios externos como DVD's, BlueRay o Cintas LTO, se llevarán a cabo los días lunes por la mañana.

h. Respaldo de Código fuente, ejecutables e instalaciones de los sistemas de información.

Se deben tener en cuenta los siguientes criterios para respaldar archivos y configuraciones de los sistemas de información:

- **En desarrollo:** Por la continuidad de las modificaciones, los backups deben realizarse de forma diaria, con copias semanales en medios externos.
- **En producción:** Dependiendo de las modificaciones realizadas o actualización de versiones, los backups deben darse cada vez que ocurra algún cambio o modificación.

NOTA: Solo personal autorizado puede tener acceso al código fuente de la aplicación; con el propósito de evitar cambios no deseados que puedan afectar el funcionamiento de la ésta.

i. Medios de instalación de software licenciado

Las copias de seguridad se realizarán solo una vez, cada que se adquiera un nuevo software. Éstas serán hechas directamente en un medio de almacenamiento externo (CD, DVD, Cintas LTO).

j. Grabaciones de las cámaras de video vigilancia.

Las grabaciones de las cámaras de video vigilancia se almacenan directamente en el servidor del dispositivo (cámara). El operador, ejecutará backups incrementales semanalmente, y deberá transferir los archivos a un disco duro externo. Los discos duros externos, almacenarán los archivos transferidos por un periodo de 90 días, después de transcurrido este tiempo, comenzará un proceso de reciclaje y liberación de espacio.

También se realizará una copia de seguridad mensual, empleando los backups incrementales, ésta se almacenará en un medio de almacenamiento externo, CD's, DVD's, Blue Ray o Cintas.



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 11 de 37

7. Políticas y Normas para el respaldo de Información

7.1 Normas del Tiempo Disponible para efectuar las copias de seguridad de la Información

Los procesos de Backup automáticos se realizarán en horas no laborables, a partir de las 11:00 P.M hasta las 6:00 A.M del siguiente día.

Las copias de seguridad que deben realizarse de forma manual, se programarán para los fines de semana, en la mañana, quedando a responsabilidad del operador, el éxito del proceso y el registro del mismo en las bitácoras de control (**Anexo 01. Formato FTI-008-01.06 – Formato FTI-012-01.06**).

7.2 Resguardo físico de los Medios de Almacenamiento Backup y Organización del Ambiente

El área de Informática debe contar con ambientes adecuados para el almacenamiento de las copias de seguridad; uno de ellos, ubicado dentro del área, y el otro, fuera de ésta, como almacén externo; con el propósito de garantizar la seguridad física de los medios empleados para la realización de los backups.

7.2.1 Normas que garantizan la seguridad física de los Backups y Medios de Almacenamiento externos

A. Realización de backups en el Servidor de Almacenamiento

1. El jefe de área o a quien delegue este, es el responsable de realizar los backups directamente en el servidor.
2. Es necesario registrar en la bitácora de control los backups realizados, que demuestren el éxito y ejecución del proceso (**Anexo 01. Formato FTI-012-01.06**).
3. El jefe del área es el responsable de designar a una persona para que realice las copias de seguridad desde el servidor de almacenamiento a un medio de almacenamiento externo, ya sea CD, DVD, BlueRay o Cintas.

B. Realización de backups en medios de almacenamiento externos

1. La persona designada por el Jefe de Informática será responsable de administrar los servicios de resguardo interno y externo de los Discos u otros medios de respaldo. Entrega o retiro de los discos, antes y después de efectuada la copia de seguridad.



(9)

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 12 de 37

Además de realizar la verificación de que el dispositivo físico de copia se encuentre en óptimas condiciones. El responsable asignado deberá guardar las copias siguiendo un orden determinado.

2. Se contarán con medios de almacenamiento externos en almacén; los necesarios para efectuar los respaldos. La persona asignada, es responsable de solicitar con anticipación el número de cintas o discos necesarios para respaldar la totalidad de la información dentro del período en curso.
3. Los backups realizados, en discos o cintas, deben estar etiquetados y ordenados, para su fácil localización, y conocer en todo momento, las últimas versiones. Las etiquetas deben usar un código sencillo, con un número de secuencia lógica, como se hace referencia en el **Anexo 02**, que muestra el modelo de etiqueta a utilizar. Las etiquetas se colocarán en la caja de protección de los discos o cintas, de manera externa, con el propósito de evitar daños o problemas de lectura.
4. Cada grupo de discos debe ser guardado en su propio contenedor, es decir, los ambientes designados como almacenes de las copias de seguridad, deben poseer unidades de almacenamiento divididos en niveles con su respectiva ubicación y etiqueta, que permita la distribución ordenada de los discos y cintas empleadas en los procesos de backup.
5. Sólo personal responsable y autorizado, tendrá acceso al ambiente delimitado como área de servidores y almacén externo. Se deben instalar dispositivos de vigilancia o sistemas de detección de intrusos, además de alarmas, que estén activas las 24 horas del día. Se debe registrar la fecha y hora de entrada y salida de los visitantes.
6. Los discos permanecerán en el almacén principal (interno) por una semana, después serán trasladados al almacén externo, por esto, es necesario establecer un control del registro de los discos o cintas, que determine el envío y recepción de backups a otro lugar fuera del ambiente principal (**Anexo 01: Formato FTI-014-01.06– Formato FTI-015-01.06**).



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 13 de 37

7. El administrador o responsable de este proceso, revisará periódicamente el ambiente donde se encuentran almacenados los Backup (interno y externo), garantizando que éste se encuentre en óptimas condiciones físicas, a temperatura adecuada, fuera de humedad, efectos químicos, vibración, radiación, etc. para evitar que los discos se dañen o sufran algún tipo de contingencia. Además es necesario, contar con equipos contra incendios, ubicados estratégicamente en ambos almacenes.

NOTA: Las personas que ingresan al almacén de copias de seguridad deben registrar sus datos personales en una bitácora de Control (**Anexo 01. Formato FTI-016-01.06**); además, en la medida de lo posible, tomando en cuenta la importancia de la información, las copias realizadas en medios externos serán **comprimidas**, como un mecanismo de seguridad.

7.3 Control del Registro de los Respaldos de Información realizados

Es necesario llevar un registro de todas las copias de seguridad realizadas, para mayor control y monitoreo de acciones (**ANEXO 01**).



7.3.1 Normas que regulan el registro de los Respaldos de Información

Registrar los respaldos de información realizadas de forma diaria, semanal, mensual o anual en la bitácora de control (**Anexo 01. Formato FTI-008-01.06– Formato FTI-012-01.06**); tomando en cuenta los siguientes datos:

- Correlativo general: secuencia del medio con respecto al número total de discos o cintas utilizadas (ID).
- Año
- Dispositivo Físico empleado.
- Frecuencia
- Fecha de generación de la copia de seguridad.
- Tipo de Información.
- Contenido: descripción precisa de los datos contenidos en el disco.
- Tipo de Backup realizado.
- Responsable asignado.



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 14 de 37

NOTA: El registro debe ser efectuado por la persona responsable de los backups en el servidor de almacenamiento y por aquella que realiza las copias en los medios de almacenamiento externos.

7.4 Restauración y comprobación de la Integridad de la Información Respaldata

Es necesario comprobar y garantizar la integridad de la información que se ha resguardado.

7.4.1 Normas de Comprobación de la Integridad de la Información

1. Toda restauración de backup solicitada debe estar autorizada por el jefe inmediato del solicitante y ser presentada por escrito como un requerimiento.
2. El tiempo estimado para la restauración de backups, tomando en cuenta la frecuencia con la que se realiza el backup, es el siguiente:
 - a. Restauración backup diario: 2 h.
 - b. Restauración backup semanal: 4 h.
 - c. Restauración backup mensual: 6 h.
 - d. Restauración backup mayor a 1 año: 2 días.
3. Se harán restauraciones de prueba cada dos meses, programadas previamente, con el fin de dar seguridad al mecanismo de restauración.
4. Toda restauración debe ser registrada en la bitácora de control (**Anexo 01. Formato FTI-013-01.06**).



7.5 Respaldo de la información de los usuarios finales

1. Toda la información importante de cada Usuario (relacionada directamente con sus labores en la Institución) deberá ser almacenada en el Servidor de Archivos, sin excepciones. Es responsabilidad del usuario, los backups y copias de seguridad que efectúe a su información.
2. La información contenida en el servidor y equipos es confidencial, por lo que se debe garantizar que solo personal autorizado tenga acceso a esta data.
3. La información almacenada de cada usuario será sometida de forma periódica a auditorías, por parte del personal del área de Informática; con el objetivo de verificar que no se utilice el

19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 15 de 37

servidor de archivos para guardar información no relacionada con las labores del usuario, como música, videos, juegos, software sin licencia, etc.

4. Para realizar los backups se deben utilizar medios externos como CD's, DVD's, BlueRay o Cintas LTO.

7.6 Normas que regulan las Responsabilidades del Personal encargado

La persona asignada como responsable de la realización de los backups en el servidor de almacenamiento y copias de seguridad en medios externos tiene las siguientes obligaciones:

Responsable de los backups en Servidor:

1. Es el responsable de la correcta generación de las copias de seguridad.
2. Es el responsable del registro, administración, seguimiento y custodia de los procesos de backups en el Servidor.

Responsable de las copias en medios de almacenamiento externo:

1. Es el responsable de la administración, seguimiento y custodia de los procesos de backups en los medios de almacenamientos externos.
2. Debe administrar correctamente los ambientes, interno y externo, previstos como almacenes de los medios físicos empleados en las copias de seguridad.
3. Debe realizar el requerimiento de los medios de almacenamiento necesarios para el periodo en curso.
4. Entregar las copias de seguridad solicitadas por el Jefe de área, en caso de auditorías o solicitudes de restauración.
5. Colocación de los discos o cintas empleadas durante los procesos de backups; además del registro de éstas en las bitácoras.
6. Debe registrar la información solicitada en las bitácoras de control (**Anexo 01. Formato FTI-008-01.06**), y en el rótulo de las cintas o discos (**Anexo 02**), para luego guardarlas, de acuerdo a su clasificación, en los almacenes provistos.



①.

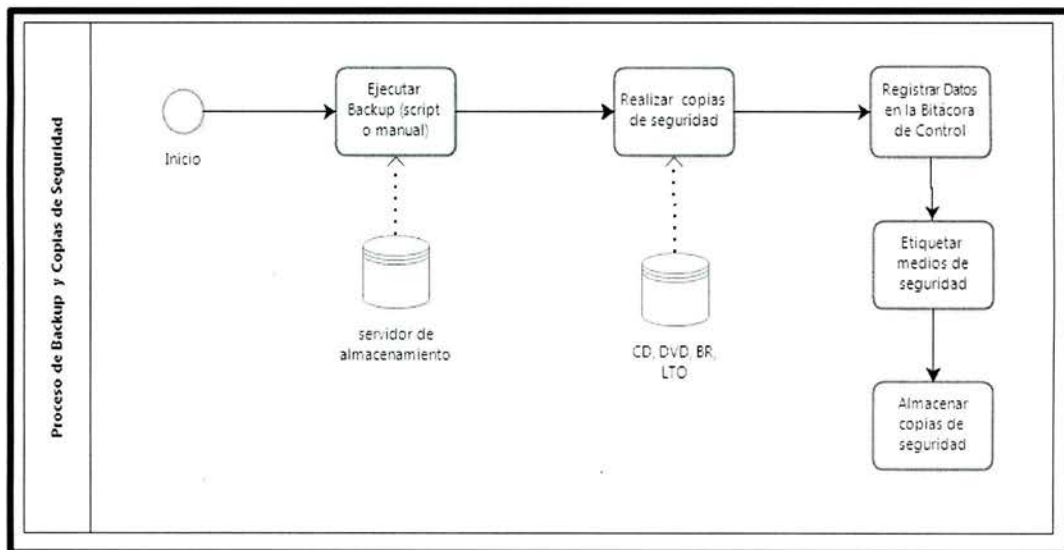
POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 16 de 37

CONTROL INTERNO

Monitorear periódicamente el cumplimiento de las políticas establecidas para el resguardo de la información, a través de la presentación de informes; donde se especifique los respaldos realizados durante un determinado periodo.

8. Procedimientos y Programación de Backup

8.1 Proceso general de Backup



POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 17 de 37

8.2 Descripción de los Procedimientos de Backup

1. Base de datos de los sistemas de información en producción

Actividad	Descripción
Proceso de Backup: Bases de datos de los sistemas de información en producción	- Se ha definido que el proceso de backup se realice de forma automática, con una periodicidad: Diaria: Backups en el servidor de almacenamiento. Semanal: Copias de seguridad en medios externos como CD's, DVD's, Blue Ray o Cintas de los backups diarios. - Los backup de datos y estructura de la base de datos deben realizarse para cada base de datos que se encuentre a cargo del centro de Sistemas; para esto, deben identificarse el número de aplicativos y/o bases de datos que se respaldarán: - Base de datos POSTGRES y MySQL (producción) - Base de datos SQL(producción) - Base de datos SIGA, SIAF - Base de datos SIMI, ACTIVOS y SISPER - Los backups se realizarán en horario nocturno, fuera del horario de trabajo para evitar interrupciones; a partir de las 11:00 p.m. de la noche hasta las 6:00 a.m. - Las copias de seguridad en medios externos, de los backups hechos durante la semana, se realizarán los días lunes por la mañana. - El/los responsables de generar los backups, tanto diarios, como semanales, deben verificar el éxito del proceso y registrarlo en la bitácora de control. (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): Fecha / "Nombre BD. Extensión". En medios externos (CD's, DVD's, etc.): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable Asignado. Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, Blue Ray, Cintas LTO.



19

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 18 de 37
	• Etiquetas. • Bitácora de Verificación y control. Normatividad: • NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.	



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 19 de 37

2. Imágenes de servidores virtuales (HyperV y VmWare)

Actividad	Descripción
Proceso de Backup: Imágenes de servidores virtuales	- Se ha definido que el proceso de backup se realice de forma manual, con la asistencia de un operador, con una periodicidad: Mensual: Backup en el servidor de almacenamiento y Copia de seguridad en un medio externo, Blue Ray. - Ante cambios o modificaciones realizadas. - Los backups y copias de seguridad se programarán para el último fin de semana del mes en la mañana, ya que, es necesario interrumpir el servicio para realizar estas tareas, evitando de esta manera, perjudicar la continuidad del trabajo realizado por los usuarios. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): Imágenes /"Nombre de Servidor"/ "Fecha + NombreServidor. Extensión". En medios externos (DVD's, BlueRay o Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento: DVD's, BlueRay, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



19

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 20 de 37

3. Directorio activo

Actividad	Descripción
Proceso de Backup: Directorio activo	1. Se ha definido que el proceso de backup se realice de forma manual, con la asistencia de un operario, con una periodicidad: • Semanal: Backup en el servidor de almacenamiento (Backups Diferenciales). • Mensual: Backup en el servidor de almacenamiento y Copia de seguridad en un medio externo, CD, DVD o Cintas (Backups Full). 2. Los backups y copias de seguridad semanales se llevarán a cabo los días viernes y el backup mensual, el último fin de semana del mes, por la mañana, a fin de evitar riesgos o dificultades a los usuarios, ocasionadas por la detención del servicio. 3. El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). 4. Etiquetado: • Servidor (dentro de la carpeta o ubicación asignada): AD / Full / "Nombre Archivo + Fecha". AD / Diferencial / "Nombre Archivo + Fecha". • En medios externos (CD's, DVD's, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: • Backup Servidor: Jefe de Área • Backup Medios externos: Responsable designado Recursos: • Equipos • Medios de almacenamiento externos: CD's, DVD's, Cintas LTO. • Etiquetas. • Bitácora de Verificación y control. Normatividad: • NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



0.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 21 de 37

4. Archivos de configuración de los servidores en producción

Actividad	Descripción
Proceso de Backup: Archivos de configuración de los servidores en producción	- Se ha definido que el proceso de backup se realice de forma manual, asistido por un operador, con una periodicidad: Mensual: Backup en el servidor de almacenamiento y Copia de seguridad en un medio externo, CD, DVD o Cintas LTO de las siguientes carpetas: - Windows: "Archivos de Programas" y la carpeta que contiene los servicios. - Linux: "etc" y la carpeta que contiene los servicios. - Los backups y copias de seguridad se realizarán el último fin de semana del mes, por la mañana, a fin de evitar riesgo o dificultades en los usuarios, al detener el servicio. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): AC / "Servidor" / "Nombre Archivo + Fecha". En medios externos (CD's, DVD's, BlueRay, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, BlueRay, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 22 de 37

5. Buzones de correo electrónico

Actividad	Descripción
Proceso de Backup: Buzones de correo electrónico	- Se ha definido que el proceso de backup se realice de forma automática, con una periodicidad: Diaria: Backup en el servidor de almacenamiento. Semanal: Copia de seguridad en un medio externo, CD, DVD o Cintas LTO. - Los backups se realizarán en horario nocturno, fuera del horario de trabajo para evitar interrupciones; a partir de las 11:00 p.m. de la noche hasta las 6:00 a.m. - Las copias de seguridad en medios externos, de los backups hechos durante la semana, se realizarán los días lunes por la mañana. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): "Fecha" / "Nombre del Buzón". En medios externos (CD's, DVD's, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, BlueRay, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 23 de 37

6. Servidor de archivos

Actividad	Descripción
Proceso de Backup: Servidor de archivos	- Se ha definido que el proceso de backup se realice de forma automática, con una periodicidad: Semanal: Backup en el servidor de almacenamiento y copia de seguridad en un medio externo, CD, DVD o Cintas LTO. - Los backups en servidor y las copias de seguridad en medios externos, se realizarán los fines de semana, por la mañana. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): Fecha / "Nombre Archivo. Extensión". En medios externos (CD's, DVD's, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



(S)

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 24 de 37

7. Repositorio de Documentos

Actividad	Descripción
Proceso de Backup: Repositorio de Documentos	1. Se ha definido que el proceso de backup se realice de forma automática, con una periodicidad: • Diaria: Backups en el servidor. • Semanal: Copias de seguridad en medios externos como DVD's, Blue Ray o Cintas de los backups diarios. 2. Los backups se realizarán en horario nocturno, fuera del horario de trabajo para evitar interrupciones; a partir de las 11:00 p.m. de la noche hasta las 6:00 a.m. 3. Las copias de seguridad en medios externos, DVD's o BlueRay, de los backups hechos durante la semana, se realizarán los días lunes por la mañana. 4. El/los responsables de generar los backups, tanto diarios, como semanales, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). 5. Etiquetado: • Servidor (dentro de la carpeta o ubicación asignada): Fecha / "Nombre Archivo. Extensión". • En medios externos (DVD's, Blue Ray, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: • Backup Servidor: Jefe de Área • Backup Medios externos: Responsable Asignado. Recursos: • Equipos • Medios de almacenamiento externos: DVD's, BlueRay, Cintas LTO. • Etiquetas. • Bitácora de Verificación y control. Normatividad: • NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



Q.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 25 de 37

8. Código fuente, ejecutable e instaladores de los sistemas de información

Actividad	Descripción
Proceso de Backup: Código fuente ejecutable e instaladores de los sistemas de información	- Se ha definido que el proceso de backup se realice de forma manual, con la asistencia de un operador, con una periodicidad: - Ante cambios o modificaciones realizadas. Las copias se realizarán, tanto en servidor como en medios extraíbles. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). - Etiquetado: Servidor (dentro de la carpeta o ubicación asignada): "Nombre S.I." / Nombre Archivo + Fecha. En medios externos (CD's, DVD's o Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



(S).

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 26 de 37

9. Medios de instalación de software licenciado

Actividad	Descripción
Proceso de Backup: Medios de instalación de software licenciado	- Se ha definido que el proceso de backup se realice de forma manual, con una periodicidad: - Ante la adquisición o renovación de un software. - El proceso de backup se realizará en horario normal de trabajo, ante la adquisición de nuevo software y previa instalación del mismo. - Las copias de seguridad se harán en medios externos como CD's, DVD's o Cintas LTO. - El/los responsables de generar los backups, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-008-01.06). - Etiquetado: En medios externos (CD's, DVD's, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: Backup Servidor: Jefe de Área Backup Medios externos: Responsable designado Recursos: - Equipos - Medios de almacenamiento externos: CD's, DVD's, Cintas LTO. - Etiquetas. - Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 27 de 37

10. Grabaciones de las cámaras de video vigilancia

Actividad	Descripción
Proceso de Backup: Grabaciones de las cámaras de video vigilancia	1. Se ha definido que el proceso de backup se realice de forma Manual, con la asistencia de un operador, con una periodicidad: • Semanal: Backup Incremental en Discos Duros Externos. Transferencia de archivos desde la consola del dispositivo (cámara de vigilancia) a un medio externo (Disco Duro). • Mensual: Copias de seguridad en medios de almacenamiento externos como CD's, DVD's, Blue Ray o Cintas. Los discos duros externos almacenarán un histórico de 90 días de backups efectuados, después de cumplirse ese periodo, empieza un proceso de reciclaje, para liberar espacio en el dispositivo. 2. Los backups y copias de seguridad se realizarán en horario laboral, entre las 7:30 a.m. y las 5:00 p.m. 3. Los backups incrementales semanales en Discos duros externos, se realizarán los días lunes por la mañana. Las copias de seguridad mensuales en discos o cintas, se harán el último fin de semana del mes. 4. El/los responsables de generar los backups, tanto semanales como mensuales, deben verificar el éxito del proceso y registrarlo en la bitácora de control (Anexo 01. Formato FTI-012-01.06 – Formato FTI-008-01.06). 5. Etiquetado: • Disco Duro externo: (dentro de la carpeta o ubicación asignada): Fecha / "Archivo. Extensión". • En medios externos (DVD's, BlueRay, Cintas LTO): Tipo de Medio de respaldo, Correlativo, año, Título, ID Contenido, Tipo de Información, ID Responsable, Fecha / Hora. Responsable: • Backup Servidor: Jefe de Área • Backup Medios externos: Responsable Asignado. Recursos: • Equipos • Medios de almacenamiento externos: DVD's, BlueRay, Cintas LTO. • Etiquetas.



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 28 de 37
	- Bitácora de Verificación y control. Normatividad: - NTC – ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.	



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática	Versión 1.0	Página 29 de 37

9. Documentos a Utilizar

- Formato de Control y Verificación del Proceso de Backups (Servidor) **(Anexo 01. Formato FTI-012-01.06)**
 - Formato de Almacenamiento de Medios de Resguardo (copias de seguridad) **(Anexo 01. Formato FTI-008-01.06).**
 - Formato de Control de Restauraciones de Backups **(Anexo 01. Formato FTI-013-01.06)**
 - Formato de Registro de Salida de Copias de Seguridad del almacén principal **(Anexo 01. Formato FTI-014-01.06).**
 - Formato de Registro de Ingreso de Copias de Seguridad al almacén externo **(Anexo 01. Formato FTI-015-01.06).**
- Formato de Registro de Acceso al almacén de Copias de Seguridad **(Anexo 01. Formato FTI-016-01.06).**



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 30 de 37

ANEXOS



①.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 34 de 37

Formato FTI-015-01.06

REGISTRO DEL INGRESO DE COPIAS DE SEGURIDAD AL ALMACÉN EXTERNO - Mes / Año

N°	Id Medio	Fecha	Hora de Ingreso	Ubicación	Responsable	Firma del Responsable



Formato FTI-016-01.06

REGISTRO DE ACCESO DE PERSONAL AL ALMACÉN DE COPIAS DE SEGURIDAD - Mes / Año

N°	Fecha	Hora de ingreso	Nombres	Actividades realizadas	Hora de Salida	Firma



②.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 35 de 37

ANEXO 02: ETIQUETA GENERAL DE LOS MEDIOS DE RESPALDO

La etiqueta que le colocará en los medios extraíbles empleados para la realización de las copias de seguridad tiene el siguiente formato:

The diagram shows a rectangular label with a dashed border. Inside the label, the text reads:

PROYECTO ESPECIAL ALTO MAYO - INFORMÁTICA

COPIA DE RESPALDO EN MEDIO FISICO

Below this, there are three options for the type of media, each with a checkbox:

CD ☐ DVD ☐ BR ☐

Below the media type options, there are several fields for identification and tracking:

ID: _____ AÑO: _____

TÍTULO: _____

ID CONTENIDO: _____ TIPO: _____

ID RESPONSABLE: _____ FECHA: _____

Callouts (pointing boxes) explain the fields:

- Correlativo General para todos los medios:** Points to the ID field.
- Seleccionar el tipo de medio de respaldo:** Points to the media type checkboxes.
- Indicar el año al que pertenece la copia de respaldo:** Points to the AÑO field.
- ID tipo de backup:** Points to the TIPO field.
- Título descriptivo a criterio del responsable:** Points to the TÍTULO field.
- ID contenido:** Points to the ID CONTENIDO field.
- Iniciales del que generó copia en medio:** Points to the ID RESPONSABLE field.
- Fecha de copia en medio:** Points to the FECHA field.



10.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0 Página 36 de 37

ANEXO 03: DESCRIPCIÓN DE CÓDIGOS

1. TABLA TIPOS DE BACKUP

Código (ID)	Tipo de Backups
1	Completo (Full)
2	Diferencial
3	Incremental

2. TABLA DE TIPOS DE CONTENIDOS

Código (ID)	Tipo de Backups
1	BASE DE DATOS POSTGRES PRODUCCION
2	BASE DE DATOS SQL PRODUCCION
3	BASE DE DATOS SIAF, SIGA
4	BASE DE DATOS SIMI, ACTIVOS Y SISPER
5	CORREO
6	PROXY
7	IMAGEN MV, SISGEDO
8	IMAGEN MV, CORREO
9	IMAGEN MV, GLPI
10	IMAGEN MV, W2K3
11	IMAGEN MV, WEBAPP 1
12	IMAGEN MV, WEBAPP 2
13	DIRECTORIO ACTIVO
14	ARCHIVOS DE CONFIGURACIÓN DE LOS SERVIDORES EN PRODUCCIÓN
15	SERVIDOR DE ARCHIVOS
16	REPOSITORIO DE DOCUMENTOS
17	CÓDIGO FUENTE, EJECUTABLES E INSTALADORES DE LOS S.I
18	SOFTWARE LICENCIADO
19	GRABACIONES CÁMARAS DE VIDEO VIGILANCIA



19.

POLÍTICAS DE BACKUPS Y COPIAS DE SEGURIDAD		
POLÍTICAS Y PROCEDIMIENTOS PARA EL RESPALDO DE INFORMACIÓN		FTI-004-01.00.06
Proyecto Especial Alto Mayo Informática		Versión 1.0
		Página 37 de 37

3. TABLA DE RESPONSABLES

Código (ID)	Tipo de Backups
MABL	MIGUEL ANGEL BEJARANO LAZO
SLLS	SARITA LLOJA SEGURA



①.