



INSTRUCTIVO DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN INSTITUCIONAL

Antiguo Cuscatlán, Octubre 2014

INDICE

I.	OBJETIVO DEL MANUAL	3
II.	ALCANCE DEL MANUAL.....	3
III.	BASE LEGAL.....	3
IV.	POLÍTICAS.....	3
1.	RESPALDO DE INFORMACIÓN.....	3
2.	Servidores físicos	3
3.	Servidores virtuales	3
4.	Frecuencia de respaldos.....	3
5.	PERIODICIDAD DE RESPALDO DE LA INFORMACIÓN DE USUARIOS.....	4
6.	RESPONSABILIDADES DE LOS USUARIOS.....	4
7.	TAREAS Y ADMINISTRACIÓN DE CINTAS DE RESPALDO.....	5
8.	RESTAURACIÓN DE DATOS	5
9.	IDENTIFICACION Y TRASLADO DE CINTAS A CAJA DE SEGURIDAD	6
10.	VIGENCIA.....	6

I. OBJETIVO DEL MANUAL

Definir las principales políticas y controles de respaldo y recuperación de datos de los sistemas de información del INSAFORP.

II. ALCANCE DEL MANUAL

El presente manual define las políticas de respaldo y recuperación de acuerdo al análisis efectuado en INSAFORP

Unidades involucradas:

- a. Gerencia de Tecnologías de la información.
- b. Unidades Organizativas que utilizan los recursos tecnológicos en la institución.

III. BASE LEGAL

Normas Técnicas de Control Interno específicas para INSAFORP, Art. 34.

IV. POLÍTICAS

El objetivo de las políticas es definir los lineamientos para realizar es respaldo y recuperación de datos institucionales.

1. RESPALDO DE INFORMACIÓN

2. Servidores físicos

Todo Servidor que se instale y configuren en ambiente de producción debe tener instalado el Software para respaldo de datos o una tarea de respaldo.

3. Servidores virtuales

Todo servidor virtual (en producción) debe a su vez contar con una tarea programada de respaldo completo y/o de forma incremental de las carpetas consideradas.

4. Frecuencia de respaldos

Esta se define según la criticidad de la información en cada servidor, por ejemplo:

Respaldo diario:

Bases de datos de sistemas

Respaldo quincenal:

Bases de datos de correo y configuraciones de servidores de correo

Respaldo Semestral:
Imágenes de máquinas virtuales

5. PERIODICIDAD DE RESPALDO DE LA INFORMACIÓN DE USUARIOS

1. En Diciembre de cada año en curso se realiza un **respaldo completo** de toda la carpeta c:\insa nombredeusuario
2. Una vez al mes se realiza un **respaldo completo** de la información almacenada en c:\insa nombredeusuarioañoencurso
3. La información institucional en las computadoras asignadas a los usuarios deben almacenarse en la carpeta C\insa nombre usuario y año en curso y es a dicha carpeta que se le realizará un respaldo diario de tipo **incremental**.

6. RESPONSABILIDADES DE LOS USUARIOS

1. El usuario debe crear cada año una carpeta con su nombre y el año en curso y dejar los otros años pasados como históricos dentro de INSA
2. El usuario con autorización del Gerente/Jefe/Coordinador de área debe notificar a través de nota, memo o help desk si tiene archivos de importancia fuera de la carpeta INSA
3. Es responsabilidad del usuario mantener toda la información de trabajo ordenada en la carpeta insa nombre usuario y año en curso
4. Es responsabilidad del Gerente/Jefe/Coordinador de área gestionar o solicitar el respaldo del equipo de personal que ha dejado de laborar en la institución
5. Los usuario no deben de colocar nombres demasiado largos a los archivos creados ya que esto ocasiona inconvenientes con las tareas de respaldo
6. Los usuarios no deben realizar más de 6 estructuras de archivos dentro de un mismo directorio debido a que esta clasificación no permite la realización de respaldo.
7. El usuario debe seguir las indicaciones de colocación de nombre de los archivos y creación de carpetas. La GTI no se hace responsable de respaldo no ejecutado debido a no aplicación de estas indicaciones.
8. El usuario no debe modificar o trabajar sobre los documentos restaurados de otro usuario que dejó de laborar en la institución, de manera que las carpetas restauradas creadas por otra persona se deben de mantener intactas.
9. El Gerente/Jefe/Coordinador de área es responsable de solicitar la restauración de respaldo histórico del personal por medio de help desk y de indicar la persona a la cual se le colocará el respaldo

7. TAREAS Y ADMINISTRACIÓN DE CINTAS DE RESPALDO

1. En los equipos de los usuarios, se deben respaldar archivos con extensión doc, docx, xls, xlsx, ppt, pptx, pfd, id y nsf
2. Las carpetas históricas de los usuarios que ya no laboran en el INSAFORP no se respaldan.
3. Diariamente se realiza el respaldo de la carpeta INSA del año en curso
4. Todos los procedimientos de respaldo deben generar un registro automático de la tarea, de manera que se permita la revisión del resultado de la ejecución de la misma
5. Los respaldos de los servidores se administran en cintas independientes a la de los usuarios
6. Antes de ejecutar cada tarea de respaldo se debe verificar el estado de la cinta a utilizar y reemplazarla en caso de que sea necesario
7. El pool de cintas se clasificará en dos categorías:
 - a. Pool de Archivo de usuarios: se respaldan los archivos de las PC de usuarios
 - b. Pool de servidores: se respaldan únicamente la información relacionada a los servidores
8. Se realiza procedimiento de reciclaje de cintas de almacenamiento al finalizar un año.
9. Al finalizar el año en curso, se debe realizar un último respaldo Full de cada carpeta INSA, el cual se debe almacenar en el banco, junto a las otras cintas de respaldo.
10. Los respaldos se deben resguardar en Cinta según la “Tabla de Sesiones”
11. En diciembre de cada año se realiza el respaldo anual de todas las carpetas \insanombredeusuario del equipo y este se envía al banco

8. RESTAURACIÓN DE DATOS

1. Aleatoriamente se deben efectuar pruebas de restauración de las copias de respaldo.
2. El usuario, mediante aprobación de Gerente/Jefe/Coordinador, puede solicitar la restauración de archivos que hayan estado ubicados en la carpeta INSA y que cumplan con la política indicada de estructura de este documento
3. El Gerente/Jefe/Coordinador de área puede solicitar la restauración del respaldo realizado del personal que ha dejado de laborar en la institución. La gerencia de TI debe restaurar en el equipo indicado la información solicitada.

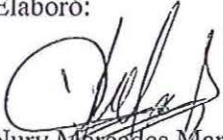
9. IDENTIFICACION Y TRASLADO DE CINTAS A CAJA DE SEGURIDAD

1. Los sitios donde se almacenan las copias de respaldo deben ser físicamente seguros, por lo que se debe llevar a la caja de seguridad del banco las cinta de respaldo.
2. Todas las copias de respaldo deben estar claramente identificadas: Sesión, Nombre de la tarea, fecha y número de cinta

10. VIGENCIA

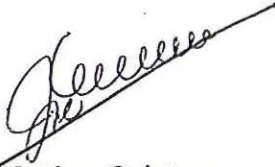
El presente instructivo entrará en vigencia a partir de su aprobación.

Elaboró:

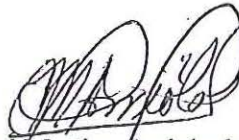


Nury Mercedes Martínez Silva
Cargo: Técnico GTI

Revisó:



José Mario Martínez Quintana
Coordinadora Unidad de Planificación



Cecyl Martiny Arriola de Hernández
Gerente de TI

Autorizó:



Ing. Carlos Gómez
Director Ejecutivo



9. IDENTIFICACION Y TRASLADO DE CINTAS A CAJA DE SEGURIDAD

1. Los sitios donde se almacenan las copias de respaldo deben ser físicamente seguros, por lo que se debe llevar a la caja de seguridad del banco las cinta de respaldo.
2. Todas las copias de respaldo deben estar claramente identificadas: Sesión, Nombre de la tarea, fecha y número de cinta

10. VIGENCIA

El presente instructivo entrará en vigencia a partir de su aprobación.

Elaboró:

Nury Mercedes Martínez Silva
Cargo: Técnico GTI

Revisó:

José Mario Martínez Quintana
Coordinadora Unidad de Planificación

Cecyl Martiny Arriola de Hernández
Gerente de TI

Autorizó:

Ing. Carlos Gómez
Director Ejecutivo

